# INFOSEC UPDATE 2001 Student Workbook

Norwich University eProtectIT Conference March 21-22, 2001



M. E. Kabay, PhD, CISSP Security Leader, AtomicTangerine, Inc.

mkabay@atomictangerine.com

at mictangerine





# 11 Breaches of confidentiality

2000-02-06 **Keywords:** bank financial system leak confidentiality windfall investors market RISKS

**Vol** 20 # 78

An error at the Reserve Bank of Australia caused e-mail to be sent to 64 subscribers of the bank's alert service informing them of a planned 0.5% increase in the prime interest rate. However, the message was sent out six minutes early, allowing some of those traders to sell A\$3B of treasury bill and bond futures -- and making some people a great deal of money.

2000-02-06 **Keywords:** confidentiality human factors workstations home computer Web browsing

RISKS, New York Times < http://www.nytimes.com/yr/mo/day/news/washpol/cia-impeachdeutch.html >

**Vol** 20 # 78

The former director of the CIA, John Deutch, kept thousands of highly classified documents on his unsecured home Macintosh computer. Critics pointed out that the system was also used for browsing the Web, opening the cache of documents up to unauthorized access of various kinds.





2000-02-20 **Keywords:** confidentiality Web site

RISKS, CNet <

http://news.cnet.com/category/0-1005-200-1550948.html >

Vol 20 # 80

H&R Block had to shut down its Web-based online tax-filing system after the financial records of at least 50 customers were divulged to other customers.

2000-02-27 **Keywords:** confidentiality mail account social security number SSN

**RISKS** 

**Vol** 20 # 82

A couple of articles in RISKS discussed the tendency of companies to put too much personal information in a single letter to their customers, thus allowing anyone intercepting the letter to impersonate them effectively. Taylor Hutt wrote about Great West's sending out name, birthdate, social security number and account number in a change-of-address confirmation; he followed up with their response to his suggestions for improvement — they accepted them! And Bob Hofkin reported that the Cigna brokerage firm resisted his efforts to improve confidentiality by telling him — a classic non-sequitur — "You're the first person to complain about this."





2000-03-17 **Keywords:** data theft credit card fraud

NewsScan (reprinted with permission)

Vol #

In January 1999, a computer vandal stole information on 485,000 credit cards from an e-commerce site and then secretly stored them in a database on a U.S. government agency's Web site. Although the theft was discovered last March when a government administrator noticed that "a lot of the memory (on the Web site) was chewed up for no reason, so he checked and found the file (containing the stolen data)," many of the credit cards remain in use today because credit card companies and card-issuing credit unions decided that it would be too much trouble to shut down the accounts and issue new numbers, according to an unnamed source. There is no evidence that the any of the cards have been used to commit fraud, and Secret Service spokesman Jim Macken says investigations point to an Eastern European perpetrator. It's unclear why the data was deposited on a government Web site, although Macken suggests that it may be the online equivalent of thumbing one's nose at U.S. authorities. (MSNBC 17 Mar 2000)

2000-03-17 **Keywords:** credit-card theft storage government police

Computerworld < http://www.nwfusion.com/news/2000/0317stopthief.html >

Vol #

In mid-March 2000, the Secret Service announced that it had tracked down a criminal hacker who stored 485,000 credit-card numbers stolen from an e-commerce Web site in January 1999. The data were stored on a Web site owned by an unnamed government agency, where they were discovered soon after they were uploaded there by the foreign criminal. Negotiations were in progress for extradition of the suspect.





 $2000\text{-}03\text{-}26 \qquad \textbf{Keywords:} \qquad \text{criminal hacker penetration credit-card theft investigation arrest} \\ \text{NewsScan (reprinted with permission), CNet} < \text{http://cnet.com/news/0-1007-200-1590629.html} > , \\ \text{FedCIRC} < \text{http://www.fedcirc.gov/news} \ge 2000.\text{html} > ... \\ \text{The permission} < \text{The per$ 

#### Vol #

Eighteen-year-old Raphael Gray was arrested Friday in Wales on charges of Internet fraud following a joint investigation by the FBI and Welsh police. Gray and an unnamed accomplice had allegedly hacked into nine e-commerce sites, stealing credit card information on 26,000 accounts in the U.S., Canada, Thailand, Japan and Britain. Among the credit cards compromised was one belonging to Microsoft chairman Bill Gates. Gray, who calls himself the "Saint of E-Commerce," said, "I just wanted to prove how insecure these sites are. I have done the honest thing, but I have been ignored." Gray and his accomplice e-mailed the credit card details to NBCi, a subsidiary of the NBC broadcasting group. (Reuters/News.com 26 Mar 2000)

http://cnet.com/news/0-1007-200-1590629.html

2000-04-28 **Keywords:** covert channel discover discarded data trash recycle access confidentiality RISKS

Vol 20 # 88

Conrad Heiney noted in RISKS that network-accessible shared trashcans under Windows NT have no security controls. Anyone on the network can browse discarded files and retrieve confidential information. [Moral: electronically shred discarded files containing sensitive data.]





2000-06-18 **Keywords:** privacy confidentiality anonymity

**RISKS** 

**Vol** 20 # 93

A RISKS correspondent reported on a new service in some hotels: showing the name of the guest on an LCD-equipped house phone when someone calls a room. Considering the justified reluctance to reveal the room number of a guest or to give out the name of a room occupant if one asks at the front desk, this service seems likely to lead to considerable abuse, including fraudulent charges in the hotel restaurant.

2000-06-24 Keywords: confidentiality concealment error vulnerability

RISKS, Wired < http://www.wired.com/news/politics/0,1283,37205,00.html >

**Vol** 20 # 93

New York Times Web-site staff chose an inappropriate mechanism for obscuring information in an Adobe Acrobat PDF document that contained information about the 1953 CIA-sponsored coup d'état in Iran. The technicians thought that adding a layer on top of the text in the document would allow them to hide the names of CIA agents; however, incomplete downloading allowed the supposedly hidden information to be read. Moral: change the source, not the output, when obscuring information.





2000-07-07 **Keywords:** e-mail domain name system DNS confusion similarity

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB962887042191508928.htm>

Vol #

One of Spain's largest banks -- and its most aggressive in terms of moving operations onto the Internet -- is suffering from an identity crisis that has resulted in thousands of messages being routed to Bulletin Board VA, run by a rural Virginia man who publishes a weekly shopper with a circulation of 10,000. Banco Bilboa Vizcaya Argentaria, which goes by the acronym BBVA after Banco Bilboa Vizcaya merged with Argentaria SA last fall, is the owner of the "grupobbva.com" domain name, but many employees, customers and outside vendors mistakenly send their sometimessensitive e-mail to "bbva.com," a domain name owned by Bulletin Board VA. "When all this e-mail started coming in, I didn't know who to contact. I didn't know who to talk to," says Bulletin Board VA owner Jim Caldwell. "To me it is beyond the stage of funny." Some of the messages contain bank account numbers and balances, and at least one contained confidential information about a possible bank acquisition. BBVA says it's in the process of changing its domain name to "bbva.es," and hopes that will solve the problem. Caldwell certainly hopes so -- he says he spends up to two hours a day clearing his server of the mislabeled messages. (Wall Street Journal 7 Jul 2000)





2000-07-13 **Keywords:** data spill confidentiality privacy e-mail address banner advertisement HTML Web page transfer

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000713/t000065732.html>

Vol #

Microsoft . . . acknowledged that a flaw in its Hotmail program . . . [was] inadvertently sending subscribers' e-mail addresses to online advertisers. The problem, which is described as a "data spill," occurs when people who subscribe to HTML newsletters open messages that contain banner ads. "The source of the problem is that Hotmail includes your e-mail address in the [Web address], and if you read an e-mail that has banner ads," the Web address will be sent to the third-party company delivering the banner, says Richard Smith, a security expert who alerted Microsoft to the problem in mid-June. Data spills are common on the Web, says Debra Pierce of the Electronic Frontier Foundation. "This isn't just local to Hotmail; we've seen hundreds of instances of data spills over the course of this year." Smith estimates that more than a million addresses may have been transferred to ad firms, but most of the big agencies, including Engage and DoubleClick, are discarding the information. (Los Angeles Times 13 Jul 2000)

2000-07-24 **Keywords:** confidentiality phone access control design flaw

**RISKS** 

Vol 20 # 97

AT&T allowed extensive details of a phone account to be revealed to anyone entering a phone number into their touch-tone interface for the Credit Management Center.





2000-08-01 **Keywords:** confidentiality customer data Web site flaw upgrade QA quality assurance RISKS, BBC < http://news.bbc.co.uk/hi/english/business/newsid\_860000/860104.stm >

**Vol** 21 # 01

Peter Morgan-Lucas reported to RISKS, "Barclays Bank yesterday had a problem with their online banking service - at least four customers found they could access details of other customers. Barclays are claiming this to be an unforeseen side-effect of a software upgrade over the weekend."

2000-08-14 **Keywords:** confidentiality Web site disclosure flaw error QA quality assurance RISKS, SecurityFocus < http://www.securityfocus.com/news/074 >

**Vol** 21 # 01

Kevin Poulson of SecurityFocus reported "Verizon's twenty-eight million residential and business telephone subscribers from Maine to Virginia had portions of their private telephone records exposed on a company web site. . . . "

2000-12-24 **Keywords:** privacy confidentiality breach credit-record data integrity RISKS

**Vol** 21 #

Beth Roberts discovered that credit bureaus were still identifying her by her former married name and sent her credit records with the address of her ex-husband. She pointed out that this could be a risk in cases of vindictive ex-spouses.





# 13.1 Data diddling

2000-01-28 **Keywords:** quality assurance financial systems data diddling Web

NewsScan (reprinted with permission), ZDNet < http://205.181.112.101/zdnn/stories/bursts/0,7407,2429909,00.html >

Vol #

As financial institutions continue to develop online innovations, . . . electronic banking got some bad news when it was discovered that the software used by the online X.Com Bank allowed customers to transfer funds from the account of any person at any U.S. bank. All they had to know was the person's account number and bank routing information. According to the company, the dollar amounts involved in fraudulent transfer were "not significant," and the security flaw has now been corrected. But security expert Elias Levy says, "Anyone with half a clue could perform these unauthorized transfers for over a month via their Web site and create some real financial problems for other people." The company's Web site boasts that its use of technology "makes accessing and moving your money easy." (New York Times 28 Jan 2000)





2000-02-10 **Keywords:** data diddling embezzlement insider employee indictment New York Times

Vol #

Tony Xiaotong Yu, 36, of Stamford, CT, was indicted on 2000-02-10 in NY State Supreme Court in Manhattan on charges of unauthorized modifications to a computer system and grand larceny. Mr Yu worked for Deutsche Morgan Grenfell Inc. from 1996 as a programmer. By the end of 1996, he became a securities trader. The indictment charges that he inserted a programmatic time bomb into a risk model on which he worked as a programmer; the trigger date was July 2000. The unauthorized code was discovered by other programmers, who apparently had to spend months repairing the program because of the unauthorized changes Mr Yu allegedly inserted.

2000-06-15 **Keywords:** data diddling grade fixing scandal bribery access control logoff failure RISKS

**Vol** 20 # 91

Peter G. Neumann reported, "At least 20 Berkeley High School seniors (hopefully, graduating) are apparently involved in a grade altering episode. The grade program is accessible to only about 20 employees, who must use \*two\* passwords. (Wow, that is REAL security!) But one of the computers was most likely left logged in and unattended. One student admitted paying \$10 for the change."





# 13.2 Data corruption

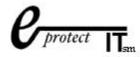
2000-01-23 **Keywords:** backup failure operations quality control data loss

**RISKS** 

**Vol** 20 # 76

Someone responsible for the US National Archives' e-mail system did not understand the concept of a backup. In 1999, it seems that a system problem deleted about 43,000 messages. The contractor responsible for making backups had not, in fact, been doing any. Finally, someone turned off system logging because it slowed down the system. The Assistant Archivist had a brilliant, if pessimistic, view of backups, saying, "the safest way to save important messages is to print them out".





2000-03-12 **Keywords:** QA quality assurance audit trail investigation grades

**RISKS** 

**Vol** 20 # 84 & 86

Mark Lutton reported in RISKS on a week-long kerfuffle at MIT, when the grades of 22 students in a cell biology class were randomly altered. Initial suspicions focused on hacking, and the teacher, Harvey Lodish, told his class on 2 March 2000 that he had uncovered a cheating scandal. On March 10, the Boston Globe reported that in fact a teaching assistant had sorted the student-name column but not all the other ones, thus failing to carry all the data through the sort. Lutton suggested, "It seems to me that bound paper ledger books would be a much better tool for keeping grade records, at least for this teacher and his assistants." [Some other ideas: (1) Enable the audit-trail feature (can create large files but does record all changes); (2) keep daily backups with version numbers so that a good version of the data can be located and used quickly.]

In a later issue of the RISKS Forum Digest (20.86), correspondents Tony Lima and John Pearson both pointed out that the fundamental problem was that the teaching team was using a spreadsheet to do a database's job. Spreadsheets have no mechanism for ensuring record integrity, whereas even simple databases can protect against the kind of scrambling that occurred in this example.

2000-07-10 **Keywords:** data corruption QA quality assurance testing

RISKS, CNN < http://www.cnn.com/2000/TECH/computing/07/10/system.crash.idg/index.htm >

Vol 20 # 95

Peter G. Neumann wrote, "Milan's stock exchange (Europe's fourth largest) opened 8 hours late on 5 Jul 2000, after corruption of the authorized-dealer database resulting from testing of a new covered-warrants market the previous evening -- evidently a maintenance glitch. Brokers claimed losses of 20 billion lire (US\$9.9M) from lost commissions. (The London exchange had an 8-hour blackout in April 2000.)"





## 14.1 Viruses

2000-01-18 **Keywords:** Microsoft Windows 2000 specific virus

Telecomworldwire, ComputerWorld < http://www.computerworld.com/home/print.nsf/all/000113DD52 >

Vol #

F-Secure announced discovery of the first Windows2000-specific virus. Win2K.Inta or Win2000.Install is a file infector. The company stated that it was not a major threat.





## **14.2** Worms

2000-01-01 **Keywords:** script worm e-mail Outlook

SecurityPortal, Computer Associates, SARC

Vol #

The Wscript.Kak was identified in late December 1999 by Computer Associates. This worm spreads through e-mail using only Outlook Express 5.0 running on Windows 98. With Internet Explorer 5 settings at low or medium, the embedded script executes automatically, without user intervention. That is, the worm replicates even if the user does \_not\_ open or preview an infected attachment. Once loaded, the worm attaches a copy of itself to every outbound e-mail message. By April 2000, this worm was the top infectious code in Europe, the Asia Pacific region and the USA.

2000-01-03 **Keywords:** worm IRC e-mail

SecurityPortal.com (reprinted with permission), <

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=VBS\_TUNE >

Vol #

Trend Micro Virus Alert: VBS\_TUNE: This worm is fast spreading and uses email (Microsoft Outlook) and IRC servers (mIRC, and PIRCH). This worm is destructive and it spreads in the same way as the Melissa virus, but unlike Melissa, VBS\_TUNE also uses IRC servers for propagation.





2000-01-15 **Keywords:** e-mail-enabled dropper worm Trojan

F-Secure < http://www.f-secure.com/v-descs/haiku.htm >

Vol #

F-Secure (formerly Data Fellows) identified another e-mail enabled worm they called Haiku. Its carrier was a detailed e-mail message about a Haiku generator which actually works. However, the worm code spreads through appropriation of the victim's e-mail address list.





2000-05-08 **Keywords:** worm e-mail malware

NewsScan (reprinted with permission)

Vol #

[The I LOVE YOU computer worm struck computers all over the world, starting in Asia, then Europe. The malicious software spread as an e-mail attachment, sending itself to all the recipients in standard e-mail address books.] Within days, there . . . [were] new variations of the destructive software program popularly known as the Love Bug because it's sent as an attachment with the words "I love you" in the subject line. In one variation, the subject line purports that the message you're receiving contains a joke, and in another you're told that the message is a confirmation notice for a Mother's Day gift order. To avoid being affected by the bug, do NOT open attachments to suspicious e-mail messages. (ZDNet 5 May 2000)

Philippine authorities . . . detained a 27-year-old man for questioning after searching the house of the suspected creator of the infamous "Love Bug" virus. The virus, called the most virulent ever created, was responsible for deleting files on computers worldwide, as it wormed its way from computer to computer using e-mail address books to target its next victims. The main suspect is said to be a 23-year-old woman living with the man who was detained, a young computer student from a middle-class family. Detectives have said it is possible that the suspect is not responsible, but her computer certainly is: "It was only [her] computer used to launch the virus that was traced but anybody could use that computer," said an official with the Philippine National Bureau of Investigation. "The user here is invisible, it could be anybody. The difference is that the person we have identified is the registered owner of that computer." (Reuters/TechWeb 8 May 2000)

[On 11 May,] Filipino computer science student Onel de Guzman of AMA Computer College in Manila . . . told authorities that he may accidentally have launched the destructive "Love Bug" virus out of "youthful exuberance." However, he would not admit that he had himself created it, saying in Tagalog: "It is one of the questions we would rather leave for the future." The name GRAMMERSoft, a computer group to which the 23-year-old man belongs, appears in the computer code of the virus, and reporters have learned that de Guzman's thesis project was rejected by AMA officials because it described a way of illegally obtaining passwords from other computer users. But investigators have not charged either de Guzman or his friend Michael Buen of any crime, nor identified them as suspects. Asked what he felt about the massive amount of damage caused around the world by the virus, de Guzman's reply was: "Nothing." (AP/San Jose Mercury News 11 May 2000)





Philippine authorities investigating the source of the "Love Bug" computer virus that originated in that country . . . [said] they have more than four principal suspects who may have been responsible for launching the virus, which destroys computer files, steals passwords, and replicates itself by sending copies of the virus to everyone in the infected computer's address book. Suspects include Onel de Guzman, a 24-year-old dropout of a computer school, and his friend Reonel Ramones, the only one of the group of suspects who will definitely be charged with criminal wrongdoing. The names of the other suspects were found on diskettes confiscated from the apartment Ramones shared with de Guzman and de Guzman's sister. (Reuters/San Jose Mercury News 12 May 2000)

2000-05-19 **Keywords:** worm e-mail enabled malware Outlook

NewsScan (reprinted with permission)

#### Vol #

A variation on the "Love Bug" computer [worm] . . . [started] going around [in May], destroying most on the files on computers it defects. Targeted at users of Microsoft's Outlook mail program, the . . . [worm] is contained in the attachment of a ".vbs" attachment arriving in an e-mail message with a subject line starting with "FW:" followed by a randomly selected name. If you receive such a message, do not open the attachment. (AP/Washington Post 19 May 2000)





2000-06-06 **Keywords:** malware worm denial of service e-mail cell phone propaganda hactivism vandals

NewsScan (reprinted with permission), MSNBC < http://www.msnbc.com/news/417066.asp>

Vol #

The first-ever computer . . . [worm] targeting cell phones is causing anxiety in Spain, where about 100 infections have been reported so far. The "I-Worm.Timofonica" virus works in much the same way as the ILOVEYOU . . . [worm] that wreaked havoc on computer systems last month — it arrives as an e-mail attachment that, when opened, sends a copy of itself to everyone in the victim's Microsoft Outlook address book. For each one of those messages, it generates a random cell phone number from a block of numbers known to be used by Spanish telecom carrier Telefonica. A short message is then sent to each mobile phone, castigating Telefonica for alleged monopolistic tendencies and questionable corporate practices. As a final insult, it also attempts to delete all files on the victim's hard drive and performs several other operations that makes restoration difficult. "Two or three viruses down the road we might see these things taking out phones," warns one security specialist. (MSNBC 6 Jun 2000)





2000-06-19 **Keywords:** worm Trojan e-mail scrap object file suffix masquerade

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/009074.htm> , San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/021805.htm>

#### Vol #

A new computer . . . [worm] called "Stages," is going around and clogging the e-mail systems of some organizations. Like the recent "Love Bug" . . . [worm] it multiplies by sending a copy of itself to everyone listed in the infected computer's address book; however, unlike that other . . . [worm], it masquerades as a ".txt" file even though it's really a ".shs" file that can contain executable and malicious code. Beware of opening the attachment of any e-mail message containing the words "funny," "life stages," or "jokes" in the subject line. (AP/San Jose Mercury News 19 Jun 2000)

[By early August,] There . . . [were] more than 200 reported cases in Japan of a computer virus called "Stages" that invades address books in the Microsoft Outlook software of computer users who open an e-mail attachment labeled Life-Stages.txt.shs. The virus apparently originated in the U.S. If you receive an e-mail attachment of that kind, do not open it. (AP/San Jose Mercury News 3 Aug 2000)

2000-08-21 **Keywords:** worm criminal hacker prosecution jurisdiction NewsScan (reprinted with permission)

#### Vol #

Deciding that new laws against computer crime could not be applied retroactively, the [U.S.] Justice Department . . . dropped charges against the former college student suspected of responsibility for unleashing the "Love Bug" computer . . . [worm] last May. Worldwide damages were estimated at up to \$10 billion. (USA Today 21 Aug 2000)





2000-11-01 **Keywords:** virus worm payload remote control e-mail Trojan dropper NASA Incident Response Center < http://www-nasirc.nasa.gov/nasa/whats\_new.html >

**Vol** # B-00-156

The SONIC worm was found in the wild on Oct 30. This nasty remote-control worm arrived by e-mail with subject "I'm your poison" and an attachment (either GIRLS.EXE or LOVERS.EXE). If the Trojan dropper is run, it installs a core process that then searches for payload instructions on a site in the GeoCities Web-hosting service. The current payload opens a backdoor to the infected system and also monitors activity, much like BackOrifice. There were already several variants in circulation by the time the worm was discovered by Kaspersky Labs. There was some hope that the original hard-coded GeoCities site could be shut down, but it was likely that other payload-supply sites would be encoded in new variants.





# 14.4 Trojans

2000-01-02 **Keywords:** Trojan e-mail password stealer

SecurityPortal.com (reprinted with permission), Symantec < http://www.symantec.com/avcenter/venc/data/pwsteal.trojan.html >

#### Vol #

PWSteal.Trojan is a Trojan which attempts to steal login names and passwords. These passwords are often sent to an anonymous email address. Symantec: PWSteal.Trojan Virus

2000-01-03 **Keywords:** Trojan operating system corruption damage

SecurityPortal.com (reprinted with permission), < http://securityportal.com/topnews/finjan19991229.html >

#### Vol #

Finjan Software Blocks Win32. Crypto the First Time: Finjan Software, Inc. announced that its proactive first-strike security solution, SurfinShield Corporate, blocks the new Win32. Crypto malicious code attack. Win32. Crypto, a Trojan executable program released in the wild today, is unique in that infected computers become dependant on the Trojan as a "middle-man" in the operating system. Any attempt to disinfect it will result in the collapse of the operating system itself. It is a new kind of attack with particularly damaging consequences because attempting to remove the infection may render the computer useless and force a user to rebuild their system from scratch.





2000-07-25 **Keywords:** impersonation Web site confidentiality password stealer Trojan horse RISKS, MSNBC < http://www.msnbc.com/news/435937.asp >

**Vol** 20 # 97

Avi Rubin contributed the following summary to RISKS: "Somebody in the Ukraine registered PayPaI.com (note the resemblance to PayPaI, especially with the upper-case I [in some fonts]), then copied PaypaI's HTML and sent mail to a bunch of PaypaI users saying 'J. Random has just transferred \$827 to you using PayPaI, log in at http://www.paypaI.com/ to claim it!' of course, as soon as you `logged in' your password was mailed to some free e-mail service."

2000-08-29 **Keywords:** Trojan mobile computers palmtop

 $News Scan \ (reprinted \ with \ permission), \ New \ York \ Times \\ < http://partners.nytimes.com/library/tech/00/08/biztech/articles/30palm-virus .html>$ 

Vol #

Software companies . . . reported that the first . . . [malware] to target the Palm operating system has been discovered. The bug, which uses a "Trojan horse" strategy to infect its victims, comes disguised as pirated software purported to emulate a Nintendo Gameboy on Palm PDAs and then proceeds to delete applications on the device. The . . . [malware] does not pose a significant threat to most users, says Gene Hodges, president of Network Associates' McAfee division, but signals a new era in technological vulnerability: "This is the beginning of yet another phase in the war against hackers and virus writers. In fact, the real significance of this latest Trojan discovery is the proof of concept that it represents." (Agence France Presse/New York Times 29 Aug 2000)





2000-10-27 **Keywords:** criminal hacker Trojan horse passwords e-mail industrial espionage source code penetration

 $News Scan \ (reprinted \ with permission), \ Associated \ Press, \ New \ York \ Times < \\ http://partners.nytimes.com/2000/10/27/technology/27WIRE-MSHACK.html > , \ Washington \ Post < http://washingtonpost.com/wp-dyn/articles/A40244-2000Oct30.html >$ 

#### Vol #

Microsoft's internal computer network was invaded by the QAZ "Trojan horse" software that caused company passwords to be sent to an e-mail address in St. Petersburg, Russia. Calling the act "a deplorable act of industrial espionage," Microsoft would not say whether or not the hackers may have gotten hold of any Microsoft source code. (AP/New York Times 27 Oct 2000)

However, within a few days, Microsoft . . . [said] that network vandals were able to invade the company's internal network for only 12 days (rather than 5 weeks, as it had originally reported), and that no major corporate secrets were stolen. Microsoft executive Rick Miller said: "We started seeing these new accounts being created, but that could be an anomaly of the system. After a day, we realized it was someone hacking into the system." At that point Microsoft began monitoring the illegal breakin, and reported it to the FBI. Miller said that, because of the immense size of the source code files, it was unlikely that the invaders would have been able to copy them. (AP/Washington Post 30 Oct 2000)





## **15.1** Fraud

2000-01-06 **Keywords:** stock manipulation fraud Web

NewsScan (reprinted with permission), New York Times < http://www.nytimes.com/library/tech/00/01/biztech/articles/06net.html >

Vol #

The Securities and Exchange Commission has filed a civil lawsuit against Yun Aoo Oh Park (known as "Tokyo Joe" on the Web site where he dispenses stock market advice), charging him with defrauding investors by selling his own shares in stocks that he was urging his readers to buy. First Amendment lawyer Floyd Abrams says: "The position of the S.E.C. is not ridiculous and cannot be blown away by hoisting a First Amendment banner, but the case does raise a serious First Amendment issue involving the continued availability of the Web as a place where people can speak broadly in an uninhibited manner about topics, including the stock market." (New York Times 6 Jan 2000)

2000-02-21 **Keywords:** stock manipulation pump and dump fraud Web site penetration RISKS

Vol 20 # 81

Peter G. Neumann wrote in RISKS: "A fake press release announced a merger of Aastrom Biosciences Inc. with Geron Inc., a California biopharmaceutical house. Aastrom stock fell, while Geron rose. Aastrom asserted that the message on their Website was totally bogus, and presumably the result of a penetration."





2000-06-09 **Keywords:** fraud misrepresentation accounting dissimulation lies investors scam NewsScan (reprinted with permission), Investor's Business Daily

#### Vol #

Shaky bookkeeping practices account for some dot-coms' inflated revenue reports, and a proposal before the Securities and Exchange Commission would put an end to accounting loopholes that enable these companies to jigger their figures. At issue is a tendency on the part of some companies to report as gross revenue the total sales price of all transactions, regardless of whether any revenue from those transactions is retained by the company. For many Web businesses that sell other companies' products, this practice has enabled them to boost their reported earnings and lure unwary investors. "This is going to impact a wide range of companies," says an Internet analyst. "Companies that report revenue one way are going to be rubbing their hands in glee. Now they can say their competitors were reporting bogus figures all along." (Investor's Business Daily 9 Jun 2000)

2000-06-29 **Keywords:** fraud deceptive advertising computers retailers

NewsScan (reprinted with permission), New York Times < http://www.nytimes.com/library/tech/00/06/biztech/articles/30free-pcs.html>

#### Vol #

Value America, Buy.com, and Office Depot, as the result of charges brought by the Federal Trade Commission that they and other retailers have been guilty of deceptive advertising of so-called "free" or low-cost personal computers, will now post real, out-of-pocket costs of computers sold with three years of Internet service. The FTC said that some consumers ended up spending \$869 for a computer advertised at \$269. Although agreeing to change their ads, the three companies do not admit to having done anything wrong, and a Buy.com executive said, "We feel like our customers understood the promotion, and we received no complaints from the customers about the advertisement being misleading." (Reuters/New York Times 29 Jun 2000)





2000-09-01 **Keywords:** fraud hoax information warfare stock manipulation securities rumors forgery

NewsScan (reprinted with permission) Investors.com < http://www.investors.com/editorial/tech05.asp>

#### Vol #

A former employee of online press release distributor Internet Wire was arrested [on the 31st of August] and charged with securities and wire fraud in connection with the distribution of a phony press release that sent a tech company's stock price plummeting last week. Shares of Emulex, a maker of fiber-optic equipment, lost up to 60% of their value, most of it during one 15-minute freefall, after some financial news services, including Dow Jones and Bloomberg, ran stories based on the release. The bogus release claimed the company had issued a profits warning, that it was being investigated by securities regulators, and that its CEO had stepped down. The stock eventually recovered most of its value after the company denied the reports. The suspect, 23-year-old Mark Jakob, allegedly used a computer at El Camino Community College to construct and send the release, and then initiated a series of trades that netted him profits of \$240,000. (AP/Investors Business Daily 1 Sep 2000)





2000-09-07 **Keywords:** fraud hoax information warfare stock manipulation securities rumors forgery

NewsScan (reprinted with permission)

Vol #

Days after arresting the California man responsible for the Emulex hoax, U.S. Securities and Exchange Commission officials conducted its fourth major "Internet sweep," taking action against 33 companies and individuals accused of using the Internet to defraud investors in classic "pump and dump" stock scams. Enforcers cited manipulation of more than 70 microcap or penny stocks, which are more loosely regulated than Big Board shares and have long been the target of illegal trading activities. "Thinly traded microcap stocks are particularly susceptible to online manipulations," says Richard H. Walker, SEC director of enforcement. "That's why we have made this area one of our highest enforcement priorities." The individuals and companies charged on Wednesday had allegedly reaped illegal profits totaling more than \$10 million. Many of the individuals had no experience in stock trading, and included a bus mechanic, a college student and a car-service driver. (Financial Times 7 Sep 2000)





2000-10-24 **Keywords:** fraud background check e-commerce dot-com firms investigation background

NewsScan (reprinted with permission), Financial Times < http://news.ft.com/news/industries/infotechnology >

#### Vol #

Internet executives are four times more likely to have "unsavory backgrounds" than execs from other industries, according to a study by corporate security firm Kroll Associates. Over the past six months, Kroll has carried out 70 due diligence background checks of dot-com executives and board members, and about 39% -- 27 people -- were found to have problems -- much higher than the typical 10% that Kroll expected. Problems included: violations of Securities and Exchange Commission rules, insurance fraud, undisclosed bankruptcies, frauds committed overseas, and even links to organized crime. In one of the most extreme cases, two people that Kroll was investigating because they had made an unsolicited offer to invest in a U.S. dot-com company were later murdered. "In the course of the law enforcement investigation they found the two were connected to penny stocks promotional scams and organized crime," says Ernie Brod, executive managing director of Kroll's New York office. Most of the problems were not associated with the inexperienced management teams who frequently run dot-coms, but rather with "gray beards" brought in to add stature to the company. "I refer to these people as vampire investors," said Brod. "Maybe they put a couple of bucks in, then they lick their lips at the opportunity and suck exorbitant consulting fees out of them, or put their relatives on the payroll." (Financial Times 24 Oct 2000)





## 15.2 Extortion

2000-01-12 **Keywords:** Web penetration extortion revenge credit-card confidentiality AP, NewsScan, PR releases, InternetNews, New York Times, Daily Telegraph (Australia)

Vol #

A 19-year-old Russian criminal hacker calling himself Maxus broke into the Web site of CD Universe and stole the credit-card information of 300,000 of the firm's customers. According to New York Times reporter John Markoff, the criminal threatened CD Universe: "Pay me \$100,000 and I'll fix your bugs and forget about your shop forever....or I'll sell your cards [customer credit data] and tell about this incident in news." When the company refused, he posted 25,000 of the accounts on a Web site (Maxus Credit Card Pipeline) starting 1999-12-25 and hosted by the Lightrealm hosting service. That company took the site down on 2000-01-09 after being informed of the criminal activity. The criminal claimed that the site was so popular with credit-card thieves that he had to set up automatic limits of one stolen number per visitor per request. Investigation shows that the stolen card numbers were in fact being used fraudulently, and so 300,000 people had to be warned to change their card numbers.





2000-01-15 **Keywords:** criminal hacker investigation extortion theft proprietary information data source code

PA, Sunday Times (London)

Vol #

In September 1999, the Sunday Times reported in an article by Jon Ungoed-Thomas and Maeve Sheehan that British banks were being attacked by criminal hackers attempting to extort money from them. The extortion demands were said to start in the millions and then run down into the hundreds of thousands of pounds. Mark Rasch is a former attorney for computer crime at the United States Department of Justice and later legal counsel for Global Integrity, the computer security company that recently spun off from SAIC. He said, "There have been a number of cases in the UK where hackers have threatened to shut down the trading floors in financial institutions. . . . The three I know of (in London) happened in the space of three months last year one after the other. . . . In one case, the trading floor was shut down and a ransom paid." The International Chamber of Commerce (ICC) confirmed it had received several reports of attempted extortion. Ungoed-Thomas and Sheehan quoted Pottengal Mukundan, ICC Director of Commercial Crime Services, as saying, "We have had cases of extortion and the matter has been investigated internally and the threat removed. . . . I don't think you will find there are many companies which admit to having a problem." Finally, the authors spoke with Edward Wilding, Director of Computer Forensics at Maxima Group; he said, "Computer extortion is not rife, but we do get called to assist in incidents where extortionists have attempted to extract money by the use of encryption and where databases of sensitive information have been stolen."

According to Padraic Flanagan of the British Press Association in mid-January 2000, UK police were investigating a dozen attempts by criminal hackers to extort funds from multinational companies in Britain.





2000-01-18 **Keywords:** criminal hacker penetration bank extortion credit card

AP, Dow Jones, RISKS

**Vol** 20 # 75

In January, information came to light that VISA International had been hacked by an extortionist who demanded \$10M for the return of stolen information — information that VISA spokesperson Chris McLaughlin described as worthless and posing no threat to VISA or to its customers. The extortion was being investigated by police but no arrests had been made. However, other reports suggested that the criminal hackers stole source code and could have crashed the entire system. In a follow-up on RISKS, a correspondent asked, "... [What source code was \*stolen\*? It is extremely unlikely that it was \*the source code for the Visa card system\* as stated! There is no such thing. Like any system, it would consist of many source libraries, each relating to different modules of the overall system. So we should be asking what source was copied? (You can hardly say it was \*stolen\*, as that would imply that it was taken away, leaving the rightful owner without possession of the item of stolen property, and we all know that is not what happens in such cases. In a shop like Visa, the code promotion system maintains multiple copies in the migration libraries, so erasure of the sole copy is highly unlikely)."





2000-01-25 **Keywords:** extortion cryptanalysis smart card counterfeit theft fraud NewsScan, MSNBC, ZDNet < http://www.zdnet.com/zdnn/stories/news/0,4586,2428429,00.html > , Crypto-Gram < http://www.counterpane.com/crypto-gram-0002.html >

#### Vol #

French programmer Serge Humpich spent four years on the cryptanalysis of the smart-card authentication process used by the Cartes Bancaires organization and patented his analysis. When he demonstrated his technique in September 1999 by stealing 10 Paris Metro tickets using a counterfeit card, he was arrested. The man had asked the credit-card consortium to pay him the equivalent of \$1.5M for his work; instead, he faced a seven-year term in prison and a maximum fine of about \$750,000 for fraud and counterfeiting (although prosecutors asked for a suspended sentence of two years' probation and a fine of approximately U\$10,000). He was also fired from his job because of the publicity over his case. In late February 2000, he was given a 10-month suspended sentence and fined 12,000 FF (~ U\$1,800).





2000-12-13 **Keywords:** penetration confidentiality credit card theft extortion

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/2000/12/13/technology/13HACK.html > , MSNBC

Vol #

The FBI . . . [began] searching for a network vandal who stole 55,000 credit card numbers from a private portion of the Creditcards.com Web site and published them on the Internet after the company refused to pay the intruder money in order to keep the information from being circulated. . . . . " (New York Times 13 Dec 2000)

The attack began in August 2000 but the revenge posting of the numbers occurred only in December. The criminal demanded \$100,000 in extortion money and also claimed on a Web site that he was trying to obtain a contract for improving network security: "Michael Butts says I need to talk to Michael Stankewitz from COO [sic]...I told him that O want to help creditcards.com, he had my price and he knew my deal," the Web page reads. "He knew what kind of information we had from their servers. I would destroy it all after the agreement was made and provide network security. Now, I didn't receive any payment from creditcards.com and I am going to make them bankrupt."





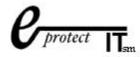
# 15.3 Slamming

2000-06-07 **Keywords:** slamming fraud unauthorized phone service contract impersonation NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/articles/A10351-2000Jun6.htm>

#### Vol #

Long-distance company WorldCom Inc. . . . [agreed to pay] \$3.5 million to settle an inquiry by the Federal Communications Commission into 2,900 complaints from persons charging that WorldCom telemarketers switched them away from other phone service carriers using a deceptive practice known as "slamming." WorldCom president Bernard J. Ebbers . . . [said] the slamming incidents "were perpetrated by a few sales employees who have since been terminated." (Washington Post 7 Jun 2000)





# 16.1 Industrial espionage

2000-01-29 **Keywords:** industrial espionage government spies surveillance eavesdropping RISKS, Sunday Times (London), < http://www.sunday-times.co.uk/news/pages/sti/2000/01/23/stinwenws03006.html?999 >

**Vol** 20 # 77

According to James Clark, writing in the Sunday Times of London, French intelligence set up at least eight listening posts focused on communications with British industries. British executives were warned to avoid discussing confidential details over unsecured phone lines, especially mobiles.





2000-06-20 **Keywords:** industrial espionage dumpster diving trashing

NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/articles/A22819-2000Jun19.html> , New York Times

< http://partners.nytimes.com/library/tech/00/06/biztech/articles/29 tech.html>

#### Vol #

Microsoft . . . [complained] that various organizations allied to it have been victimized by industrial espionage agents who attempted to steal documents from trash bins. The organizations include the Association for Competitive Technology in Washington, D.C., the Independent Institute in Oakland, California, and Citizens for a Sound Economy, another Wash., D.C.-based entity. Microsoft . . . [said], "We have sort of always known that our competitors have been actively engaged in trying to define us, and sort of attack us. But these revelations are particularly concerning and really show the lengths to which they're willing to go to attack Microsoft." (Washington Post 20 Jun 2000)

#### ORACLE DEFENDS TRASHING OF MICROSOFT

Saying he was exercising a "civic duty," Oracle chairman and founder Lawrence J. Ellison defended his company of suggestions that Oracle's behavior was "Nixonian" when it hired private detectives to scrutinize organizations that supported Microsoft's side in the antitrust suit brought against it by the government. The investigators went through trash from those organizations in attempts to find information that would show that the organizations were controlled by Microsoft. Ellison, who, like his nemesis Bill Gates at Microsoft, is a billionaire, said, "All we did was to try to take information that was hidden and bring it into the light," and added: "We will ship our garbage to [Microsoft], and they can go through it. We believe in full disclosure." "The only thing more disturbing than Oracle's behavior is their ongoing attempt to justify these actions," Microsoft said in a statement. "Mr. Ellison now appears to acknowledge that he was personally aware of and personally authorized the broad overall strategy of a covert operation against a variety of trade associations." (New York Times 29 Jun 2000)





2000-07-06 **Keywords:** industrial espionage international investigation law enforcement surveillance interception monitoring e-mail eavesdropping

NewsScan (reprinted with permission), Newsbytes < http://www.newsbytes.com/pubNews/00/151697.html>

#### Vol #

The European Parliament has renewed its attack on the U.S.-devised Echelon satellite and eavesdropping network by forming a "temporary committee" to investigate whether the spy network was used for commercial espionage against European businesses. The parliament said the committee will also determine Echelon's legality. Echelon, which is jointly operated by the U.S., the U.K., Australia, Canada and New Zealand, is capable of intercepting phone, fax and e-mail signals around the world and is intended to gather intelligence regarding terrorist and other threats to the U.S. and its allies. (Newsbytes 6 Jul 2000)

2000-08-06 **Keywords:** information warfare insider industrial espionage lawsuit intellectual property IP

 $News Scan \ (reprinted \ with \ permission), \ Washington \ Post < http://www.washingtonpost.com/wp-dyn/articles/A46353-2000 Aug6.html>$ 

#### Vol #

Qwest . . . [sued] AT&T following an AT&T threat to take legal action to prevent an AT&T employee from leaving it to work for Qwest. AT&T . . . [said it was] concerned that the employee -- a vice president of policy and law -- would make use of AT&T's confidential information or trade secrets, but a Qwest executive . . . [countered]: "I think AT&T may be trying to slow the flow out of the company and show people it's not going to be easy to leave." (AP/Washington Post 6 Aug 2000)





# 16.2 Industrial information systems sabotage

 ${\bf 2000\text{-}01\text{-}09} \qquad \textbf{Keywords:} \qquad \text{Web site hacked vandalized Trojan horse quality assurance technical}$ 

support

RISKS

**Vol** 20 # 74

Someone posted a message on the Intuit UK server that claimed to be offering an update to Quicken: "There is an upgrade available to updated [sic] your current version of Quicken 2000. Would you like to download the update now? Don't be afraid, it is just a test: My name is Nour." RISKS Forum correspondent Stephen Page wrote, "Either test code has leaked into live service or their site has been hacked. In either case, it is a serious security breach for software which is trusted (e.g., a Trojan horse could create access to users' personal financial data)."

2000-01-19 **Keywords:** criminal hacker insider sabotage Web

Wall Street Journal

Vol #

Global Health Trax Inc. reported that its old Web site was opened to unauthorized access in January, possibly because of sabotage by disgruntled employees. Although there was no evidence of penetration, detailed account information about hundreds of distributors was unprotected for several hours, including bank account and credit card numbers.





Vol #

In 1998, Sun Microsystems accused Microsoft of corrupting its implementation of Java to reduce the platform-independence of their product -- a violation of Microsoft's license agreement. In January 2000, a federal court judge reinstated a suspended injunction barring Microsoft from distributing its modified version of Java to other software developers.





2000-02-02 **Keywords:** sabotage software Trojan denial of service Internet access information warfare

NewsScan (reprinted with permission); < http://www.washingtonpost.com/wp-dyn/business/A60549-2000Feb1.html> , < http://www.washingtonpost.com/wp-dyn/business/A23076-2000Feb7.html>

#### Vol #

A Maryland attorney has filed a class-action suit against America Online, charging that version 5.0 of its software changes computer settings of users who try to upgrade from earlier versions and making it no longer possible for them to just click on the desktop icon of another Internet service provider to access the Internet. The attorney says that that AOL is in effect forcing the customer into behavior shaped to suit the company rather than the computer user, and complains: "The Internet is supposed to be like free speech, with open access." (Washington Post 2 Feb 2000)

[A few days later,] Three Washington-area Internet service providers have filed a class-action suit America Online charging that customers who install AOL's new version 5.0 software and choose it as the default browser find that their computer setting are changed in a way that makes it much harder to access providers that use other browsers, thereby allowing AOL to leverage its market position "to foreclose competition and gain unfair competitive advantage." Although not a party to the lawsuit, Prodigy is demanding compensation from AOL for the administrative and technical costs it incurred helping customers who found it difficult to access their Prodigy accounts after installing AOL version 5.0. An AOL executive says that lawsuits are without merit and insists: "We're not doing anything that other ISPs aren't doing." (Washington Post 8 Feb 2000)

#### YET ANOTHER "MONOPOLY"? AOL SUED BY SMALL ISP

[In April,] Galaxy Internet Services Inc., a small Internet service provider in Massachusetts, . . . [sued] America Online, charging that it "attempted to eliminate competition in the Internet service market" when it introduced new software (AOL 5.0) that blocks AOL subscribers from using other Internet service providers. About 8% of America Online subscribers also use some other ISP, and Galaxy is hoping to be joined it its suit by other competitors of AOL. (Reuters/San Jose Mercury News 4 Apr 2000)





2000-02-10 **Keywords:** sabotage design quality assurance information warfare NewsScan (reprinted with permission), WP < http://www.washingtonpost.com/wp-dyn/business/A31920-2000Feb9.html>

#### Vol #

Looking into complaints by end-users, small computer businesses and Microsoft rivals, the European Union on Wednesday launched a probe into allegations that Microsoft is bundling its new Windows 2000 operating system with other software in such a way that only its own products are fully interoperable, placing rivals at a disadvantage. Microsoft, which is still embroiled in a U.S. antitrust suit, denies the charges, claiming it has complied with EU competition law. If the EU finds the allegations to be true, it could force Microsoft to make changes to the operating system, or face fines of up to 10% of global revenues if it failed to do so. Microsoft, the world's biggest software company, earns nearly a quarter of its revenues in Europe. (Reuters/Washington Post 9 Feb 2000)

2000-02-23 **Keywords:** Web vandalism penetration criminal hacker prosecution

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/080797.htm>

#### Vol #

Ikenna Iffih, a 28-year-old computer science student at Northeastern University has been charged with hacking his way into government and military computers and disrupting the operations of an Internet service provider in the state of Washington. If convicted, he will face up to 10 years in prison and a fine of \$250,000. Prosecutors say that Iffih caused "substantial business loss, defacing a Web page with hacker graphics, copying personal information, or in the case of a NASA computer, effectively seizing control." (AP/San Jose Mercury News 23 Feb 2000)





2000-04-12 **Keywords:** industrial espionage denial-of-service lawsuit sabotage dc.internet.com < http://dc.internet.com/news/article/0,1934,2101\_342551,00.html >

**Vol** 20 # 76

In the long-running lawsuit by Moore Publishing against Washington law firm Steptoe & Johnson, LLP, United States District Judge Thomas Pennfield Jackson denied a defense motion to quash the lawsuit in mid-April. A report from < dc.internet.com> summarized the allegations as follows: "The suit claims an employee of Steptoe & Johnson used the stolen e-mail identity of a former client to launch and attempt to cloak the origins of a denial of service attack designed to overwhelm the Moore Publishing sites and server with bogus requests to prevent access by legitimate consumers and computer users." The attacks were discovered in August 1999; when the victim notified the apparent originators of the penetrations, the denial-of-service attacks began in high volume.

2000-08-01 **Keywords:** sabotage intellectual property IP information warfare lawsuit NewsScan (reprinted with permission)

Vol #

Motorola . . . filed a federal lawsuit charging that its copyrights were infringed when the eBay online auction site was used to sell Motorola radio service software that allows personal computers to program two-way radios. A Motorola lawyer . . . [said], "We don't see any reason why pirates should benefit when our loyal customers are doing what they are supposed to do." (Reuters/New York Times 1 Aug 2000)





# 16.3 Infrastructure protection

2000-02-17 **Keywords:** information warfare investigation denial-of-service government policy law enforcement legislation

Reuters, AP

Vol #

In the wake of the distributed denial-of-service attacks, US federal officials debated the appropriate responses to the high-profile interference with e-commerce. Attorney General Janet Reno said publicly on 2000-02-07 that the attacks were a "wake-up call" to improve Web security and to catch criminal hackers. However, she did not endorse proposals by FBI Director Louis Freeh to prosecute criminal hackers under US anti-racketeering statutes. She did strongly support criminal prosecution, however: "We've got to help define, by our prosecutions based on real crimes, what you can and can't do on the Internet," she said.

2000-02-19 **Keywords:** information warfare infowar study panel conference

UPI

Vol #

At the American Association for the Advancement of Science (AAAS) meeting in Washington, DC, panelists from government and from private industry concurred that information warfare is a real threat to the United States. Speakers urged better cooperation among law enforcement officials around the world to catch the culprits responsible for attacks on systems and network; they also supported changes in international law to allow extradition of suspects. Skeptics such as Kevin Poulson scoffed that if the infrastructure were as vulnerable as infowar proponents claimed, we'd have no electricity.





2000-02-24 **Keywords:** law enforcement federal agency infrastructure protection NewsScan (reprinted with permission), MSNBC < http://www.msnbc.com/news/374361.asp>

Vol #

U.S. Attorney General Janet Reno . . . nixed a bipartisan Senate plan that would make a single federal agency responsible for securing all federal computer networks against cyber-sabotage. The proposed legislation, sponsored by Sen. Fred Thompson (R-Tenn.) and Sen. Joseph Lieberman (D-Conn.) would centralize oversight authority within the Office of Management and Budget. Without commenting directly on the plan, Reno said that fending off cyber-attackers will depend more on chips and circuits rather than who's in charge: "It is not just a matter of centralizing a particular function in a particular office, it is a matter of developing the technology to protect the technology, but to do so consistent with our constitutional rights." (APBNews.com 24 Feb 2000)

2000-02-29 **Keywords:** infrastructure protection law enforcement government private industry Internet security

NewsScan (reprinted with permission)

Vol #

Technology leaders are discouraging too much government involvement in online security. Howard Schmidt of Microsoft says that infrastructure security "does not lend itself to government management. The private sector has the knowledge and expertise to help fight against computer crimes on the infrastructures on which they operate." And Charles Giancarlo of Cisco Systems insists that "the technology industry showed that it can respond swiftly and effectively, taking steps to quickly beat back the attacks to make it harder for similar assaults to succeed in the future." But the view of Deputy U.S. Attorney General Eric Holder is that some private security will fail, and he says: "In such cases, law enforcement must be prepared and equipped to investigate and prosecute cybercriminals in order to stop their criminal activity, to punish them and to deter others who might follow in their path." (AP/USA Today 29 Feb 2000)





2000-03-03 **Keywords:** government initiative infrastructure protection law enforcement safeguards

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cth501.htm>

Vol #

A new presidential directive [was]... issued requiring U.S. government agencies to assess their vulnerability to cybervandalism. Chief of Staff John Podesta will work the agencies to put together a government-wide plan, and President Clinton says, "We must do more to uphold Americans' high expectations that their right to privacy will be protected online." (Bloomberg/USA Today 3 Mar 2000)

2000-04-26 **Keywords:** infrastructure information warfare intrusion attack real-time process control

RISKS, < http://www.techserver.com/noframes/story/0,2294,500197283-500270387-501418162-0.00.html >

**Vol** 20 # 87

Steve Bellovin wrote in RISKS, "The Associated Press reports that hackers, in conjunction with an insider, penetrated computer systems belonging to Gazprom, the Russian gas monopoly. . . . What is especially interesting about this case is that they managed to take control of the system controlling the flow of gas in pipelines, according to the Russian Interior Ministry. This makes it one of the few confirmed incidents of direct cyberthreats to a country's infrastructure."





2000-06-18 **Keywords:** air traffic control disruption failure infrastructure protection information warfare simulation

RISKS, BBC < http://news.bbc.co.uk/hi/english/uk/newsid\_796000/796018.stm] >

**Vol** 20 # 93

Peter G. Neumann wrote, "On 17 Jun 2000, thousands of would-be passengers were stranded when the main air-traffic control computer collapsed. The National Air Traffic Services computer was fixed later in the day, but the resulting congestion caused many people to spend the night at airports around the UK, and many flights were cancelled the next day as well. Heathrow and Gatwick were hardest hit, although other UK airports experienced severe delays. This was the second time in a week that the computer system had failed." [MK notes: consider this an information warfare simulation that supports the view that critical infrastructure protection truly is important.]

2000-07-06 **Keywords:** critical infrastructure emergency phone service backhoe attack cable availability

**RISKS** 

**Vol** 20 #

Mark Richards reported on how a backhoe operator sliced through a major Bell Atlantic phone cable, cutting service not only to several thousand subscribers but also the local 911 emergency operators. The outage lasted several days.





2000-07-31 **Keywords:** Internet connectivity topology availability infrastructure protection information warfare communications disruption

**RISKS** 

Vol 20 #

Researchers from Notre Dame University discovered that concerted attack on the most highly-connected nodes of the Internet would fragment the Net into non-communicating subsets.

2000-09-25 **Keywords:** information warfare critical infrastructure protection book

**RISKS** 

Vol 21 # 07

The security world was rocked to its foundations when revered book reviewer Rob Slade published a favorable review of controversial writer and speaker Winn Schwartau's latest book, \_Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption \_ [Thunder's Mouth Press, ISBN 1-56025-246-4]. Slade wrote, "s some may know, Winn Schwartau and I do not see eye-to-eye on the emphasis to be given to certain exhortations in alerting the public to matters of computer security. So when he informed me of his latest book, he noted that I might like to do the usual hatchet job on it. Unfortunately, I can't fully comply. While I may quibble with some aspects of his latest book, overall it is a good overview of the existing computer security situation, and would make a helpful introduction for new computer and Internet users. . . . While there is a heavy emphasis on the sensational, overall this book does provide the security novice with a fairly reliable picture of the current security environment. Possibilities are generally presented as such, and the analysis of relative dangers is usually good. A number of useful tips are given that can help home and small business computer users be more secure in their computer and network use. Security specialists will find little that is new here, but that is not the target audience for the book. I have frequently been asked for a recommendation for a general security introduction directed at the nontechnical computer and Internet user, and, for all its flaws, I think this work may be the closest I've seen. "





2000-12-08 **Keywords:** government policy information warfare national security NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cti892.htm >

#### Vol #

In August, Richard Clarke, the National Security Council's first Infrastructure Coordinator, called on industry to strengthen their own information security as a means of strengthening national security: "By protecting the IT security of your company, you can protect the security of your country." He listed several ways the US government is trying to improve information security:

- \* Supporting Information Sharing and Analysis Centers (ISACs), which are industry-specific groups of companies sharing information about INFOSEC;
- \* Possibly amending the FOIA (Freedom of Information Act) to reduce ISAC participants' fears of being forced to reveal sensitive information if they talk to government and law-enforcement officials about cybercrimes;
- \* Supporting INFOSEC research by spending \$600M, especially in areas not immediately attractive to the private sector;
- \* Sharing classified information with "trusted partners."

Speaking at a computer security conference [in December], National Security Council member Richard Clarke told the audience that the next president of the U.S. should appoint (and get Congressional confirmation of) a government-wide chief information officer with authority to oversee all of the government's security. ''What this presidential election year showed is that statistically improbable events can occur. It may be improbable that cyberspace can be seriously disrupted, it may be improbable that a war in cyberspace can occur, but it could happen.'' Clarke said that certain other nations have created information-warfare units and are "creating technology to bring down computer networks." (AP/USA Today 8 Dec 2000)





# 16.4 Military perspectives on INFOWAR

2000-02-19 **Keywords:** information warfare Central News Agency, Taipei via BBC Monitoring

Vol #

The Taiwan Research Institute warned that the country should gird itself against information warfare by the People's Republic of China. Elements of IW, they explained, included disruption of critical infrastructure, disruption of military communications, command, control and intelligence (C3I) operations, and misinformation campaigns to damage economic activity and lower morale on the island before initiating conventional warfare.

2000-06-24 **Keywords:** virus worm information warfare disclosure espionage bungling error mistake

RISKS, The Times of London < http://www.the-times.co.uk/news/pages/sti/2000/06/18/stinwenws01024.html >

**Vol** 20 # 93

Monty Solomon summarized a report in The Times of London about an information warfare experiment gone wrong: "Bungling NATO scientists have created a computer virus "by mistake", causing military secrets to find their way onto the internet. The virus, called Anti-Smyser 1, was created by scientists at NATO'S Kfor peacekeeping force headquarters in Pristina, Kosovo. They were seeking protection from virus attacks similar to those launched at NATO by the Serbs during the Kosovo conflict. But the experiment went wrong, and scientists accidentally unleashed the virus on themselves. The virus, which plucks documents from the hard drives of computers and sends invisible attachments to e-mails, recently resurfaced at the Czech ministry of defence."

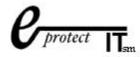




2000-07-13 **Keywords:** unstable operating system operations production RISKS, ACM Ubiquity < http://www.acm.org/ubiquity/views/m\_kabay\_3.html > **Vol** 20 # 95

Much derision resulted from the announcement on 13 July 2000 that the US Navy would be using Windows 2000 for critical control systems on a new nuclear-powered aircraft carrier. [See "Monty Python's Flying Circus: Microsoft and the Aircraft Carriers" (2000-08-15) on the ACM Ubiquity Web site for your editor's comments.]





## 16.5 Hacktivism

2000-01-19 **Keywords:** criminal hackers hacktivists political Web vandalism attacks ideology politics denial of service

AP, Newsbytes

Vol #

According to the Seattle Host Organization that organized the World Trade Organization meetings in Seattle (1999-11-30/12-03), hackers probed their Web site 700 times and tried to penetrate defenses 54 times. Attackers briefly forged the WTO's own Web site to close at one point. On the last day of the meetings, the Web site was subjected to an unsuccessful denial-of-service attack by a group calling itself the "Electrohippies."

2000-01-31 **Keywords:** political hactivism Web vandalism damage defacement propaganda NewsScan, New York Times <

http://www.nytimes.com/library/tech/00/01/biztech/articles/31japan.html >

Vol #

In the last days of January 2000, political activists (hacktivists) defaced and damaged Japanese government and business Web sites in protest for the failure of Japan to admit responsibility for the Rape of Nanking (also called the Nanjing Massacre) of 1937. Some sites (e.g., that of the National Personnel Authority) suffered major data destruction; others (e.g., Posts and Telecommunications Ministry, Government Data Research Center) saw propaganda messages added to their content. The Bank of Japan reported that its Web site was attacked 1,600 times in a single day. The attacks stimulated concern that Japanese enterprises as a whole were failing to implement effective network and Web security.





2000-02-17 **Keywords:** information warfare INFOWAR Web attacks vandalism

AP

Vol #

Throughout Latin America, cybervandals went on a rampage in the weeks following the high-profile distributed denial-of-service attacks that hit prominent Web sites in the US e-commerce community. Many of the criminal hackers posted propaganda about the Elian Gonzalez case. Security experts commented that the INFOSEC situation in South and Central America is even worse than in the US and Europe, with few sites adequately protected against intrusion and limited knowledge of computer security among law enforcement authorities there.

2000-02-17 **Keywords:** INFOWAR information warfare hactivism politics international conflict Balkans

AP

Vol #

In the Balkans, the ancient hostilities among different communities continued to have cyberspace repercussions. Armenian and Azerbaijani criminal hackers vandalized Web sites run by various organizations in each others' countries. Accusations flew through the news media about misinformation campaigns and one group, the Armenian hacker collective calling itself Liazor, actually changed the text in newspaper articles. "It wasn't a punitive action, we simply wanted to oppose spreading computer vandalism," said a Liazor spokesman, Gevork. [Hmm, opposing vandalism by vandalism. . . . Is that like having intercourse for virginity? Killing for peace?]





2000-02-18 **Keywords:** international conflict information warfare INFOWAR China Japan propaganda law enforcement censorship

AP

Vol #

According to the Associated Press, the Chinese government shut down an anti-Japanese Web site whose sponsors, allegedly the "China Extreme Right Wing Anti-Japanese Alliance", were urging cyberwar against Japan in the wake of revisionist right-wing claims that the Nanjing Massacre of 1937 never happened. The criminal hackers had put up lists of their victims; among the sites allegedly penetrated were Web sites of the Edogawa Women's University, the Management and Coordination Agency, Japan's Science and Technology Agency, the Mainichi Shimbun newspaper, and many other commercial sites.

2000-02-19 **Keywords:** criminal hackers vandalism Web idiots cretins fools stupid jerks EFE (Spanish News Agency)

Vol #

Criminal hackers bewildered Mexican government officials in the state of Chiapas by vandalizing their Web site in mid-February with pro-Zapatista slogans and also leaving FREE KEVIN graffiti behind. "Kevin? Kevin who?" was the essence of the officials' reactions. Ironically, Kevin Mitnick was released from prison on 2000-01-21.





## 17.1 Penetration

2000-01-09 **Keywords:** criminal hacker sabotage vandalism sentence trial judgement RISKS, NewsScan, USA Today < http://www.usatoday.com/life/cyber/tech/ctg955.htm >

Vol 20 # 73

In New Rochelle, NY, a former volunteer for AOL technical support was sentenced to one year in jail for breaking into AOL and causing \$50K in damages. Jay Satiro, 19, was described by his own lawyer as, "a disturbed young man." After pleading guilty of computer tampering, he was barred from having a computer in his room or computer access in his home. Judge M. Perone's severity may have been influenced by Satiro's having committed the latest offence while on probation for having used forged money orders to buy computers.

2000-01-12 **Keywords:** criminal hacker penetration intrusion passwords theft cracking youth child adolescent

NewsScan, Los Angeles Times < http://www.latimes.com/business/20000112/t000003535.html >

Vol #

A 16-year-old boy from the Global Hell gang of criminal hackers was arrested in Eldorado, CA for allegedly stealing user IDs and passwords for 200,000 of the ISP run by Pacific Bell. Police reported that the boy had decrypted 63,000 of the passwords. The lad boasted about his exploits in a chat room; apparently he may have been the hacker responsible for 26 other break-ins, including a computer at Harvard University.





2000-03-23 **Keywords:** criminal hacker informer vandal sabotage government NewsScan (reprinted with permission)

Vol #

Twenty-seven-year-old Max Ray Butler of Berkeley, California, has been indicted on charges of breaking into and causing damage to government computers belonging to such agencies as NASA, the Argonne National Labs, the Brookhaven National Lab, the Marshall Space Center, and various facilities of the Department of Defense. Butler (also known as "Max Vision") has in the past been an FBI source, helping the Bureau solve computer crimes. (AP/San Jose Mercury News 23 Mar 2000)

2000-07-13 **Keywords:** criminal hacker penetration misuse misappropriation arrest complain charges court credit-card theft gang

**RISKS** 

**Vol** 20 # 95

Keith Rhodes contributed the following summary to RISKS: > A 20-year-old man was arrested Wednesday for allegedly breaking into two computers owned by NASA's Jet Propulsion Laboratory and using one to host Internet chat rooms devoted to hacking. Raymond Torricelli of New Rochelle, N.Y., was named in a five-count complaint that also charged him with sending unsolicited advertisements for a pornographic Web site and intercepting passwords and usernames traversing networks of computers owned by Georgia Southern University and San Jose State University. He was also accused of stealing credit card numbers that were used to make more than \$10,000 in unauthorized purchases. Court papers, which were unsealed in Manhattan federal court, alleged Torricelli was the head of a hacker group known as "#conflict" and that he used the name ``rolex.'' [Source: Reuters, 12 Jul 2000]<





2000-09-11 **Keywords:** penetration credit card information theft Web site RISKS

**Vol** 21 # 04

Peter G. Neumann wrote, "Western Union warned thousands of online customers on 9 Sep 2000 that hackers had broken into the company's Web site. Although no fraudulent transactions or breaches of personal information had been discovered, the penetration could have affected on-line users. More than 10,000 customers were being alerted, suggesting they cancel their credit and debit cards. The Web site was out of service that evening, and was expected to remain that way for several days."

2000-09-22 **Keywords:** criminal hacker penetration damage trusted computing base trial punishment sentence judgement juvenile

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/2000/09/22/technology/22AP-HACK.html>

Vol #

A sixteen-year-old Florida boy . . . [was] sentenced to six months in a federal detention center for having used the Internet to break into government computers, including ones operated by NASA and the Pentagon. Attorney General Janet Reno said, "Breaking into someone else's property, whether it's a robbery or a computer intrusion, is a serious crime." (AP/New York Times 22 Sep 2000)





2000-10-04 **Keywords:** penetration fraud spoofing Web insider bank theft arrest wiretap RISKS

**Vol** 21 # 08

In Sicily, police arrested 21 alleged cyberthieves who were in the process of stealing half a billion dollars (2 trillion lira) from the Banco de Sicilia. According to news reports, the gang included members of the Mafia, computer specialists and bank employees. Thanks to wiretaps, the perpetrators were stopped before they could complete their money transfers. Their plans were reported to include attacking the bank of the Vatican.

2000-12-06 **Keywords:** hospital medical records confidentiality privacy intrusion penetration hack

RISKS, SecurityFocus < http://www.securityfocus.com/news/122 >

Vol 21 # 14

Kevin Poulson, writing in SecurityFocus, broadcast a report about a catastrophic failure of security, a criminal hacker from the Netherlands was able to penetrate the admissions records for over four thousand cardiac patients at the University of Washington Medical Center in Seattle. The records were exposed to the Internet without firewalls or any other defenses. Compounding the problem, administrators who discovered the hack penetration in mid-July, a month after they began, were apparently unaware that the records had been copied and failed to notify law enforcement officials. Despite initial refusal by UWMC technical staff to believe the reports, Poulson provided them with irrefutable evidence of the penetration: their own data.





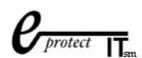
 ${\bf 2000\text{-}12\text{-}23} \qquad \textbf{Keywords:} \quad \text{penetration public relations response open frank}$ 

**RISKS** 

**Vol** 21 # 16

Egghead.com discovered a potential breach of their customer databases during a hacker penetration of their system. The company immediately published a warning to its customers as a precaution. [MK comments: The frank, open response was a refreshing change from stonewalling and concealment that unfortunately characterizes so much of corporate and government reactions to security breaches.]





# 17.2 Web vandalism

2000-01-17 **Keywords:** Web site vandalism defacement criminal hackers

AP

Vol #

In mid-January 2000, the "Lamers Team" criminal hackers claiming to be from Europe defaced the "Thomas" Web site of the Library of Congress, one of the most popular government sites among journalists and others needing information about pending legislation in the House and Senate of the USA.

2000-01-18 **Keywords:** Web defacement vandalism criminal hackers

Irish Times

Vol #

Cybervandals damaged the Web site of the University of Limerick; the perpetrators left electronic graffiti with the initials of Trinity College Dublin prominently displayed, perhaps in an attempt to implicate that institution in the crime.

2000-03-07 **Keywords:** Web defacement vandalism impersonation spoofing

**RISKS** 

**Vol** 20 # 83

In early March, someone attacked two victims in one case of Web vandalism. The Gallup Organization's Web site was defaced and AntiOnline's John Vranesevich was fraudulently indicated as the defacer. This case supports the view that it is unwise to assume that the apparent attacker really has caused the damage at hand; it makes immediate vigilante revenge action ever less reasonable.





2000-04-05 **Keywords:** Web attack law enforcement deterrence arrest search warrant seizure evidence ISP

**RISKS** 

**Vol** 20 # 87

Ulf Lindqvist reported in RISKS that the operators of the Web site for the Swedish National Board of Health and Welfare

(Socialstyrelsen) reported an attack to the National Police Computer Crime Squad so promptly that the police were able to find the perpetrator's home phone number from the ISP involved. Armed with a search warrant, they arrested a 16 year-old boy and seized his and his parents' computers. Lindqvist wrote, "What I personally find noteworthy in this story is how quickly the police reacted and that it could be a sign of the trend to treat computer crimes no differently than "low-tech" crime. When organizations see that it actually helps to call the police in cases like this, maybe they will be less reluctant to do so. The deterrent effect on would-be criminals by likely detection and immediate response should not be underestimated."

2000-09-13 **Keywords:** Web site vandalism hactivism

**RISKS** 

**Vol** 21 # 05

Mike Hogsett reported in RISKS as follows: > Someone identified as "fluxnyne" cracked into the OPEC Web site, posting this message: "I think I speak for everyone out there (the entire planet) when I say to you guys to get your collective a\*\*es in gear with the crude price. We really need to focus on the poverty-stricken countries, who don't even have enough money for aspirin, let alone exorbi[t]ant prices for heating oil. I think the lives of children are paramount to your profits."<





# 17.3 Phreaking

2000-10-12 **Keywords:** telephone calling card fraud personal identification number PIN keyspace brute-force cracking

**RISKS** 

**Vol** 21 # 09

Peter Reith, a minister in the government of Australia, repaid \$950 in calls placed by his son using an official government calling card. The minister had foolishly given his son the personal identification number (PIN) for the card. However, he expressed surprise at the 11,000 phone calls made from 900 locations around the world (e.g., the US, Singapore, Malaysia, Hong Kong, Thailand and China) which generated over A\$50,000 in charges. Fergus Henderson commented in RISKS, "in order to make phone calls billed to the card, you only need to know the 8-digit card number and the 4-digit pin number."





# Theft of equipment (laptops, ATMs, computers, cables, network components)

2000-03-24 **Keywords:** laptop portable computer theft law enforcement intelligence RISKS, BBC < http://news.bbc.co.uk/hi/english/uk/newsid\_688000/688814.stm >

Vol 20 # 85

In Britain, an MI5 agent stopped to help someone at an Underground (subway) station and got his laptop stolen. Luckily, the data were encrypted. However, Steve Loughran, writing in RISKS Forum, correctly warned that file-level encryption (e.g., the encrypting file system in Windows 2000) does not necessarily encrypt file names, so some data may be revealed by induction if overly-descriptive file names are used. [An amusing detail for non-British readers was the description of the laptop in the BBC report: "The 2,000-pound laptop was snatched as the agent stopped to help. . . . ." which raised eyebrows of those who were thinking of pounds Avoirdupois instead of pounds Sterling.]

2000-05-22 **Keywords:** laptop computer stolen secrets confidentiality theft

RISKS; The Mirror < http://www.sundaymirror.co.uk >

Vol 20 # 89

In early May, a British Navy intelligence officer lost a laptop computer containing "details of a top secret 250-billion-pound

Anglo-US super-lethal stealth Strike fighter project. . . . " The machine was recovered by The Mirror newspaper two weeks later.





2000-09-18 **Keywords:** industrial espionage information warfare theft laptop disk encryption user interface

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/ap/docs/412258l.htm>

#### Vol #

After addressing a national business journalists' meeting in Irvine, California, Qualcomm chief executive Irvin Jacobs found that someone had stolen his laptop computer, which he left on the floor of a hotel conference room. The thief acquired not only an IBM ThinkPad but also the Qualcomm secrets it contains, because Jacobs had just finished telling the audience that the slide-show presentation he was giving with his laptop contained proprietary information that could be valuable to foreign governments. People in the area "included registrants, exhibitors and guests at our conference, hotel staff and perhaps others.'' Qualcomm, a leader in the wireless industry, and is the world's leading developer of a technology known as CDMA, which makes high-speed Internet access available on wireless devices. (Reuters/San Jose Mercury News 18 Sep 2000)

In a RISKS commentary on this case, encryption expert Camillo Sars of F-Secure Corporation commented on often-ignored risks from real-time encryption of disk files:

- \* damage to a block or an entire file from flipping a single bit in the ciphertext;
- \* loss of the key and therefore of all encrypted data.

Sars ended with the comment, ". . . I second Ross Anderson's view that a paradigm shift is required. Let's not only make systems that are easier to use correctly. Let's make systems that are difficult to use incorrectly."





# 19.1 Software piracy

2000-05-05 **Keywords:** intellectual property copyright violation theft counterfeit warez criminal hackers juveniles investigations arrests

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB957492236169474418.htm>

Vol #

The FBI has arrested 17 people, five of them former or current employees of Intel, on charges of involvement with Internet sites devoted to pirated software. The five were described as having held low-level engineering jobs, and an Intel spokesman said four out of the five were no longer with the company. All 17 suspects were members of a loosely organized group called Pirates with Attitudes, which operated one of the Internet's oldest "warez" sites — a term describing a hacker variation of software sold in stores by merchants. Most warez sites are run as hobbies and their users are often teenage boys who view downloading a pirated software program to be a rite of passage. The indictments do not allege that the perpetrators were attempting to make money through their activities, but the potential penalties include a US\$250,000 fine and five years in prison. "This is the most significant investigation of copyright infringement involving the use of the Internet conducted to date by the FBI," says a spokeswoman for the Bureau's Chicago office. "It demonstrates the FBI's ability to successfully investigate very sophisticated online criminal activity." (Wall Street Journal 5 May 2000)





2000-08-17 **Keywords:** intellectual property IP wireless communications software sabotage copyright infringement violation

NewsScan (reprinted with permission)

Vol #

[In August,] America Online . . . [said] that an unauthorized distribution of its new software for wireless devices . . . [posed] no danger to the privacy of AOL users, though about 10,000 people . . . download the software from the Web in . . . [a] few days. Carnegie Mellon University computer science professor Mahadev Satyanarayanan thinks the release of the software (code-named Gamara, for the flying turtle monster that battled with Godzilla) could give clues about how to hide out on AOL's systems. Gamara uses Mozilla, a browser made by Netscape, which was purchased by AOL in 1998. (Washington Post 17 Aug 2000)





# **19.2 Music**





2000-05-05 **Keywords:** copyright infringement violation illegal copies counterfeit music files theft lawsuit ruling penalty

NewsScan (reprinted with permission); Los Angeles Times

- < http://www.latimes.com/business/20000505/t000042406.html> ; San Jose Mercury News
- < http://www.sjmercury.com/svtech/news/breaking/merc/docs/010346.htm>

#### Vol #

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)





Category 19.2 Music
Copyright © 2001 M. E. Kabay. All rights reserved.

2000-09-25 **Keywords:** intellectual property IP copyright violations infringements music band owners money profits

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/025084.htm>

#### Vol #

Although The Grateful Dead is famous for allowing its fans to make and swap personal recordings of its live concerts, the group has never authorized bootlegged copies of its studio recordings and has never allowed anyone to sell a tape of a concert, not even for the price of the tape itself. Grateful Dead's attorney, Eric Doney, says: "They have always been vehement about this: If someone is going to make money, it should be them. The music belongs to the creators, not someone else." (AP/San Jose Mercury News 25 Sep 2000)

2000-10-02 **Keywords:** intellectual property IP copyright violation infringement music distribution law bill proposal regulation decriminalization

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/2000/10/02/technology/02NECO.html>

#### Vol #

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)





Category 19.2 Music
Copyright © 2001 M. E. Kabay. All rights reserved.

2000-10-02 **Keywords:** intellectual property IP copyright violation infringement music distribution ethics popular opinion feeling survey study attitudes

NewsScan (reprinted with permission), E-Commerce Times < http://www.ecommercetimes.com/news/articles2000/001002-1.shtml>

#### Vol #

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)

2000-10-18 **Keywords:** music copyright infringement violations agreement lawsuit NewsScan (reprinted with permission), San Jose Mercury News <

http://www.mercurycenter.com/svtech/news/breaking/internet/docs/527752l.htm >

#### Vol #

Under the terms of a tentative 3-year agreement between the National Music Publishers' Association and online music company MP3.com, MP3 will pay music publishers as much as \$30 million to reimburse them for past uses of their music and to make advance royalty payments on future uses. MP3's 80,000 album collection was originally created without the permission of the publishers and recording companies that own the copyrights to the music. (Reuters/San Jose Mercury News 18 Oct 2000)





Category 19.2 Music
Copyright © 2001 M. E. Kabay. All rights reserved.

## 19.3 Movies

2000-01-26 **Keywords:** DVD encryption cracking cryptanalysis copyright prosecution teenager

NewsScan, New York Times

< http://www.nytimes.com/library/tech/00/01/biztech/articles/26disc.html>, AP

#### Vol #

Jon Johanson, a 16-year-old Norwegian boy, and his father Per Johanson were charged with violating copyright after they created and distributed a cracking program to decode DVDs (digital versatile disks) so they could be copied illegally and played on computers. The family computers were seized by police pending trial.

2000-07-21 **Keywords:** cryptanalysis cracking DVD scrambling hackers free speech litigation lawsuit

< http://www.nytimes.com/library/tech/00/07/cyber/cyberlaw/21law.html >

#### Vol #

The ongoing legal battle between the owners of movies on DVDs and criminal hackers who distributed the DeCSS program that allows unauthorized computer access to the copy-protected materials had a visitor from Norway in late July: Jon Johansen, the 16-year-old who wrote DeCSS with two other hackers in 1999. Mr Johansen's testimony was dismissed as irrelevant by the attorneys for the plaintiffs, but the judge wearily allowed the youngster to speak. "The man is here from Norway. I may as well hear it," he said. Mr Johansen's father Per said that his son was carrying on a proud tradition as a freedom fighter. [Helping people make illegal copies of movies is equivalent to fighting the Nazis??]





2000-10-03 **Keywords:** unexpected consequences movie copyright violation theft volume downloads astronomical invoices

RISKS, The Register.com < http://www.theregister.co.uk/content/1/13668.html >

**Vol** 21 # 08

An enthusiastic computer-game fan placed illegal copies of a fancy advertisement on his Web site -- one version at 45 Mb and the other at 32Mb. In July, at least 1400 people downloaded one or other of the files for a total of 62Gb of traffic; in August, downloads totaled even more (the exact number is in doubt). Since "Cannibal Harry" had a contractual limit of 500 Mb per month of data transfers included in his Web page service, his ISP slapped him with an invoice for \$6,000 for the month of July and a \$24,000 invoice for August.





# **19.4 Games**

2000-07-20 **Keywords:** intellectual property IP copyright infringement piracy lawsuits auctions Web sales

NewsScan (reprinted with permission)

Vol #

Sega . . . shut down more than 60 illegal Web sites and 125 auction sites selling pirated versions of its Dreamcast games, which until recently had been viewed as a "Fort Knox of online intellectual properties" — protected by far more sophisticated technology than the relatively simple music, film and video files targeted by services like Napster and Scour. Despite the security precautions, several dozen Dreamcast titles were released this month on the Internet and have been traded via networks like Internet Relay Chat (IRC). Charles Bellfield, Sega's director of communications, says his company's actions mark one of the first times that the Digital Millennium Copyright Act of 1998 has been invoked to go after the Web-hosting companies and ISPs used by pirate traders. "It is the first time that this act has been used not just to stop piracy, but also physical sales over the Internet. It is the first time that Webhosting companies and Web auction sites are being held accountable for the contents of what is being sold." (Reuters 20 July 2000)





# 19.5 Credit-cards, other tokens

2000-01-29 **Keywords:** credit card fraud theft counterfeit shoulder surfing confidentiality RISKS

Vol 20 # 77

The Japanese department store, Takashimaya, was victimized by counterfeiters who passed so many forged store credit cards that the chain issued 300,000 new credit cards to customers to reduce the thefts. There was some evidence that criminals systematically engaged in shoulder surfing to collect card numbers.

2000-03-14 **Keywords:** cryptanalysis cracking smart card forgery

The Guardian (London) <

http://www.guardianunlimited.co.uk/international/story/0,3604,230435,00.html >

Vol #

After Serge Humpich was punished by the French courts for demonstrating that he could fool smart-card terminals into giving him Paris subway tickets, criminal hackers released an algorithm on the Internet which they claimed would allow anyone to forge bank cards. However, Roland Moreno, a cryptographer who worked on the smart-card algorithms that slashed French bank-card fraud by 90%, described the claims as fraudulent and offered a 1M FF reward (~ U\$150,000) to anyone demonstrating that the supposed formula actually worked.





# 19.6 Legal or business documents

2000-12-05 **Keywords:** counterfeit government agency corruption insider fraud arrests criminal RISKS

**Vol** 21 # 14

Paul Nowak wrote in RISKS about another contributor to identity theft: counterfeit drivers' licenses and photo IDs: "Thus far, 14 people have been indicted -- including four AZ Motor Vehicle Division customer service employees and an Arizona Department of Transportation computer information worker. Several more arrests are expected, with more arrests expected. Four groups are accused of issuing bogus licenses and ID cards, at a cost over \$1000 each. `Buyers apparently included criminals, illegal immigrants and motorists with suspended or revoked licenses.' [Source: Article by Senta Scarborough, \*The Arizona Republic\*, 25 Nov 2000]"





# 19.7 Plagiarism

2000-01-19 **Keywords:** plagiarism forgery theft intellectual property attribution detection plagiarism

Edupage, New York Times < http://www.nytimes.com/library/tech/00/01/circuits/articles/20chea.html >

Vol #

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 antiplagiarism sites have popped up on the Web to help academics pounce on students who plagiarize 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 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.]





# 19.8 Products (hardware, clothing etc.)

2000-01-15 **Keywords:** counterfeit fake computer equipment mouse mice organized crime Los Angeles Times

Vol #

Police in the Los Angeles area seized 23,000 fake Microsoft computer mice worth around \$1M. Investigators were pursuing leads that pointed towards involvement of organized crime. The devices looked authentic (except for one batch with "Certificates [sic] of authenticity"), down to serial numbers, bar codes and boxes with authentic logos.





# 1A3 Biographical notes on individual criminals

2000-01-21 **Keywords:** criminal hacker incarceration prison jail release probation DOW JONES BUSINESS NEWS

Vol #

Criminal hacker icon Kevin Mitnick was released from prison on 2000-01-21 on parole, instructed to stay away from computers, software, modems, cell-phones and Internet-connected devices for the next three years. These conditions would make it difficult for Mitnick to enroll in college for a degree in computer science, as he desired.





2000-07-13 **Keywords:** criminal hacker parole restrictions censorship

NewsScan (reprinted with permission), CNet < http://www.nytimes.com/cnet/CNET\_0\_4\_1951220\_00.html> , < ://news.cnet.com/news/0-1005-200-2250843.html?tag= st.ne.ron.lthd.ni>

#### Vol #

Ex-convict network hacker Kevin Mitnick, out on parole but forbidden by the court to write or speak about the computer industry, is being represented by New York attorney Floyd Abrams, an expert on the First Amendment to the Constitution, which guarantees freedom of speech. Abrams has been retained by publisher Steven Brill, who wants to use Mitnick as a columnist for the Contentville Web site. (CNet/New York Times 25 May 2000)

[In July,] Kevin Mitnick. . . . won the right to pursue computer-related work. . . . [A] federal judge agreed that the restrictions were overly broad. Among the jobs now approved are: writing for Steven Brill's online magazine Contentville, speaking in Los Angles on computer security, consulting on computer security, and consulting for a computer-related TV show. Mitnick spent five years in prison after the FBI fingered him in a series of attacks on companies, including Motorola, Novell, Sun Microsystems and the University of Southern California. (AP/CNet 13 Jul 2000)





2000-09-21 **Keywords:** criminal hackers penetration civil law indictment conviction sentencing

settlement court law legal proceedings judgement punishment fine pump-

and-dump stock fraud interception wiretapping

**RISKS** 

Vol 21 # 06

Peter G. Neumann summarized three legal cases involving computer fraud and abuse:

On 20 Sep 2000, Jonathan Lebed, 15, settled a federal civil-fraud process, agreeing to pay \$272,826 for perpetuating bogus information on the Internet that led to the stock fluctuations in Just Toys Inc. and The Havana Republic and profiting therefrom.

On 21 Sep 2000, Jonathan James (cOmrade), 16, pleaded guilty to two counts of juvenile delinquency and was sentenced to six months detention for having penetrated DoD and NASA computer systems, intercepting 3,300 e-mail messages and stealing passwords. (He was 15 at the time. If he had been an adult, he reportedly would have received a sentence of at least 10 years.)

On 21 Sep 2000, Jason Diekman, 20, was charged with cracking into university (including Harvard, Stanford, and Cornell) and NASA computer systems, and stealing hundreds of credit-card numbers to buy thousands of dollars of clothing, stereo equipment, and computer hardware.

2000-09-28 **Keywords:** criminal hacker social engineering advice legitimation

NewsScan (reprinted with permission) MSNBC < http://www.msnbc.com/news/469018.asp>

Vol #

Infamous hacker Kevin Mitnick, in his first public speech since his release from prison last January, warned information technology directors that the key to network security is vigilance, detection and quick reaction. "You should adopt the mantra, 'In God we trust. Everybody else is suspect.' People are the weakest link when it comes to security, and an important question to ask yourself is not if, but when, is your e-business going to be targeted?" (ZDNet 28 Sep 2000)





# **1A4** Publications

2000-01-06 **Keywords:** criminal hacker phone phreak physical security social engineering lying cheating misrepresentation forgery trickery deceit

HackCanada < http://www.hackcanada.com/ice3/misc/telaccess.txt >

Vol #

A criminal hacker calling itself "~ Wizbone '99" published a new edition in January 2000 of an unfortunately excellent guide to social engineering that, I regret to say, bears reading by security specialists. "Gaining physical access to Server and Telecom rooms (v2.1)" < http://www.hackcanada.com/ice3/misc/telaccess.txt > summarizes the ways criminals can fool security and other personnel and gain access to restricted areas in the workplace. The writer recommends forging documents, having work shirts embroidered with the name of a fictitious firm, and other ways of lying convincingly. One of the obviously missing elements in the document is any sign that the author realizes that what (s)he is doing is wrong. The well-known principles of physical security are reinforced by the experience of this criminal: choose and train your security guards well, keep employees aware of their responsibility to report suspicious activity, communicate among different sectors of the organization, and accompany visitors and contractors at all times in secure areas.





2000-02-18 **Keywords:** criminal hackers psychology script kiddies motivations culture denial-of-service attacks

**WASHINGTON POST** 

Vol #

Libby Copeland published an interesting overview of the culture clash between older criminal hackers who espouse the hacker ethic and the script kiddies they think are ruining hacking's image. She interviews some hackers who claim never to actually use the techniques they invent — it's all an intellectual game, they say. One hacker is quoted as saying, "The people who are developing attacks and posting them, I don't consider them evil. . . . They're really doing quality control."





# 1B1 Adult pornography

2000-07-08 **Keywords:** pornography wireless application protocol WAP NewsScan (reprinted with permission)

Vol #

Analysts say the appearance of the first WAP (wireless application protocol) pornography sites signals the adoption of WAP technology into the mainstream. Although the sites offer only tiny grainy images of naked Japanese models, sociologists say that the key to predicting whether a new technology will take off is to determine whether it's used for pornography: "It's inevitable, I suppose, that with any new technology people will use it for porn," . . . [said] David Birch, CEO of Consult Hyperion. "That's been the story with photography and video cameras." The news should be welcomed by wireless companies, which have reported slower growth rates than they had hoped. (The Independent 8 Jul 2000)





2000-08-25 **Keywords:** pornography scam fraud credit-card international jurisdiction criminals theft

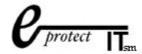
NewsScan, RISKS, E-Commerce Times < http://www.ecommercetimes.com/news/articles2000/000824-4.shtml >

**Vol** 21 # 03

The Federal Trade Commission has filed a lawsuit against Crescent Publishing Group and 64 affiliated companies that operate adult Web sites, accusing them of charging customers for services advertised as "Free Tour Web Sites." Like many adult sites, the Crescent sites requested that users supply credit card information to verify they were of legal age to view pornographic material. Customers who'd been promised a free online peep show say they were then billed for recurring monthly membership fees ranging from \$20 to \$90. Included among the complainants were some people who said they'd never visited the sites at all—in fact, one woman who'd been charged a recurring fee for several months didn't even own a computer. To add to the confusion, the charges were made under different company names. Instead of finding a charge from Highsociety.com on their statements, consumers would find charges from "Online Forum," or "Hoot Owl," or "Knock Knee." The FTC has classified the scam as one of the largest it's ever seen on the Internet, generating \$141 [million] in the first 10 months of 1999 alone.

RISKS correspondent Lenny Foner noted the folly of using credit cards as a form of age authentication.





# 1B2 Child pornography

2000-01-17 **Keywords:** child pornography kiddie porn vigilante legal action criminal hacker vandalism destruction evidence law enforcement

Computerworld

Vol #

In mid-December 1999, a group of activists and technology experts formed Condemned.org, dedicated to eradicating child pornography, pedophile sites and child exploitation on the Internet. The group uses legal means such as notifying law enforcement and system administrators of the presence of child porn on their servers; most immediately terminate the accounts responsible. However, the group warns, if there is no action taken, some of the members turn to illegal tactics. In such cases, members will hack into vulnerable sites and wipe entire hard drives. Some opponents of child pornography protest that these illegal methods destroy the evidence needed by law enforcement to locate and prosecute malefactors.





2000-11-16 **Keywords:** pornography fraud children trickery metatags

NewsScan (reprinted with permission), Financial Times < http://news.ft.com/news/industries/media >

#### Vol #

[In November, an article in the Financial Times reported that pornographers were] using "metatags," the labels attached to Web pages that identify their contents, to draw visitors seeking information on the holiday season's most popular toys, with the result that children surfing the Web for My Little Pony, Barbie or Muppets could find among their choices not only toy retailers but such sites as www.picturesofanalsex.com. Envisional, a UK company that specializes in searching the Net for trademark violations, said it has found nearly 12,000 examples of toy names being used this way. A British attorney noted that using registered trademarks in this way is illegal, as is using metatags to drive children toward obscene material, but that such laws were difficult to enforce, given the worldwide reach of the Internet. (Financial Times 16 Nov 2000)





# 1B3 Pedophilia, kidnapping, Netadoption fraud

2000-06-09 **Keywords:** children pedophiles attacks kidnap parental responsibility abduction infants

NewsScan (reprinted with permission)

Vol #

Child safety experts warned the U.S. congressional committee on child online protection . . . [on 8 June] that with the average of age of online users declining, children increasingly are put at risk by their careless or ignorant online activities. Parry Aftab, a children's advocate, told committee members that 3,000 children were kidnapped in the U.S. last year after responding to online messages posted by their abductors. A recent survey of teenage girls found 12% had agreed to meet strangers who'd contacted them online. Children between the ages of two and seven are among the fastest growing user cohorts. (Financial Times 9 Jun 2000)

2000-08-03 **Keywords:** pedophile statutory rape conviction sentencing San Jose Mercury News

Vol #

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.





# 1B5 Gambling

2000-02-14 **Keywords:** gambling stupidity gullibility consumer cheating fraud law NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/library/tech/00/08/biztech/articles/11gambling.html>

#### Vol #

The future of online gambling could be decided in a trial . . . [that started in February and pitted] the U.S. Justice Department against the World Sports Exchange (www.wsex.com), an online betting operation based in Antigua. The importance of the case goes beyond gambling, however, says one Internet attorney: "This is an interesting case of asserting jurisdiction over overseas Web sites in a criminal context. It will be closely followed by companies doing business on the Internet, both in the U.S. and abroad." The attorney prosecuting the case maintains that where the bet is placed physically doesn't matter; the crime occurs when an "interstate wire communication facility" like the Internet is used to transmit the wager. But Internet legal experts disagree, pointing out that legislation aimed at banning Internet gambling has not yet been passed in the House of Representatives. "This pushes the concept of jurisdiction to its limits," warns Henry Judy, a member of the American Bar Association's committee on cyberspace law. (Financial Times 14 Feb 2000)

[In August,] A co-owner of an online offshore gambling business based on the Caribbean island of Antigua . . . [was] sentenced to 21 months in a U.S. prison for violating . . . [that] country's federal Wire Wager Act, which makes it illegal to use telephone lines in interstate or foreign commerce to place sports bets. The prosecutor noted: "An Internet communication is no different than a telephone call for purpose of liability under the Wire Wager Act." (Reuters/New York Times 11 Aug 2000)





2000-02-28 **Keywords:** online gambling fraud

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/wires/wbusiness/20000228/tCB00V0457.html>

#### Vol #

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 [in 1999], which would make it illegal to bet on casino-style games online. A companion bill [was] pending in the House and [would] be the subject of a subcommittee hearing on March 9. (AP/Los Angeles Times 28 Feb 2000)

2000-02-29 **Keywords:** online gambling fraud prosecution conviction lawsuit international NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000229/t000019506.html>

#### Vol #

The first defendant to stand trial in New York for online gambling via offshore locations has been convicted. Jay Cohen, a U.S. citizen, ran an Antigua-based sports betting parlor called the World Sports Exchange. He was found guilty under a federal law against using telephone lines to place illegal wagers. Cohen faces up to five years in prison on a conspiracy charge and two years for each of seven sports betting counts. (Bloomberg/Los Angeles Times 29 Feb 2000)





2000-07-14 **Keywords:** online gambling fraud legislation proposal law

 $News Scan \ (reprinted \ with \ permission), \ New \ York \ Times \\ < http://partners.nytimes.com/library/tech/00/07/biztech/articles/14gamble.html> \ , San \ Jose \\ Mercury \ News < http://www.sjmercury.com/svtech/news/breaking/ap/docs/206358l.htm>$ 

#### Vol #

Legislation was introduced in July in the US House of Representatives to ban Internet gambling. [However,] The U.S. House of Representatives gave the Internet gambling industry a victory by failing to muster the two-thirds majority set as a requirement by House leaders in its 245 to 159 vote on a bill to ban online casinos. The votes in favor of the ban fell 25 short of the requirement. Sue Schneider of the Interactive Gaming Council said: "It appears that cooler heads have prevailed here. We have a brand new medium we're dealing with. We don't have the same kind of borders we had before." But Rep. Robert Goodlatte (R-Va.), who sponsored the bill, scoffed at the notion that it was anti-Internet: "One way to promote the Internet is to make sure that the seamy side of life is dealt with on the Internet. Just like child pornography has to be dealt with on the Internet, so does unregulated, out-of-control, illegal gambling." (AP/San Jose Mercury News 17 Jul 2000)





2000-10-13 **Keywords:** online gambling legislation jurisdiction

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB971401767656792229.htm >

#### Vol #

For the first time, an online-gambling site has received approval to operate in the U.S. The Nevada Gaming Control Board has okayed Virtgame.com's plan to run an online betting parlor for football games, horse races and other sports. "Twenty-four hours is one of the beauties of the Internet," says a book manager for Coast Resorts, which owns four Las Vegas casinos, "but it could be a monster to manage." Virtgame has a contract with Coast to provide the computer system for Coast's online sports-betting sites, and is now marketing its system to others in the gambling business, including state lotteries. States have jurisdiction over all types of gambling within their state lines, but federal laws still prohibit transmitting bets over state lines. (Wall Street Journal 13 Oct 2000)

2000-12-06 **Keywords:** lottery ticket purchase online gambling

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com >

#### Vol #

Lottery players in Maryland will soon be able to buy their tickets online, making Maryland the first in the U.S. to offer online ticket sales. The new service is "just the beginning in gaining access to this large and demographically desirable market niche," said the Maryland Lottery director. "The Internet will be a big factor in the future of lotteries." Maryland players will need to file an online application, and can then choose their games, numbers and the number of weeks to participate. Charges for the tickets will still have to be paid by check or money order because it's illegal in Maryland to pay for lottery subscriptions by credit or debit cards. (Wall Street Journal 6 Dec 2000)





# 1B6 Auctions

2000-01-25 **Keywords:** credit card fraud theft online auction

ZDNet < http://www.zdnet.com/zdnn/stories/news/0,4586,2427490,00.html >

Vol #

A new scam involving online auctions and an offshore bank was reported in January. Steps in the fraud:

- \* Scam artist advertises expensive electronics on auction site and posts specific price as well for direct sale.
- \* Buyer agrees to purchase equipment.
- \* Thief proposes to send equipment directly to buyer's address in return for pledge to wire price to bank if product is OK.
- \* Using the buyer's detailed information (name, address, phone number), thief opens account with Web retailer.
- \* Arranges to ship equipment to buyer but pays for product using a stolen credit-card number.

#### **Results:**

- \* Buyer now has stolen equipment in possession.
- \* Owner of stolen credit-card has expensive charge for product never received.
- \* Thief has money in offshore bank.





2000-02-15 **Keywords:** online auction fraud investigation suspicion gullibility naive consumers cheating

NewsScan (reprinted with permission), Financial Times

#### Vol #

The Federal Trade Commission is launching an assault on online auction fraud, a problem that prompted 10,000 complaints last year, up from 107 in 1997. The agency plans to train law enforcement officers, educate the public and prosecute more offenders, but notes it lacks the jurisdiction to protect the rights of U.S. citizens who purchase items from overseas Web sites. Many online auction companies have responded by saying they will cooperate with FTC efforts: eBay, for example, will begin routing complaints about its vendors directly to the FTC this week. (Financial Times 15 Feb 2000)

2000-05-04 **Keywords:** online auction fraud tax international law jurisdiction NewsScan (reprinted with permission)

#### Vol #

A Paris court . . . barred French consumers from participating in online auctions unless they use a state-approved auctioneer and pay the French value-added tax. The ruling came in response to a lawsuit filed by the association of Paris auctioneers (commissaires priseurs) against online upstart Nart.com, the first company to auction off high-priced art work on the Net. Nart does not require its buyers to pay the tax, because its auctions are handled by a subsidiary incorporated in New York, with sales paid in U.S. dollars to a U.S. bank. The French court ruled the sales were illegal, because the activities were tantamount to the "organization of auctions of objects located in France." Nart says it will appeal the ruling: "This is almost like saying that French people should not be allowed to walk into Christie's or Sotheby's in New York and bid for something on sale there," says Nart co-founder Antoine Beaussant. (Financial Times 4 May 2000)





2000-06-07 **Keywords:** online auction fraud shill misrepresentation investigation

NewsScan (reprinted with permission), New York Times

< http://partners.nytimes.com/library/tech/00/06/biztech/articles/07ebay-fraud.htm>

#### Vol #

The Federal Bureau of Investigation . . . launched an investigation of several sellers in eBay auctions suspected of "shilling" (the practice of running up a bidding price through fraudulent bids by the seller or the seller's friends). The inquiry was prompted by a . . . New York Times article about a California lawyer who almost sold an abstract painting for \$135,805, after starting the bid at 25 cents. Shilling is forbidden by eBay rules, and eBay is using its proprietary "shill hunter" software to review bidding by users. (New York Times 7 Jun 2000)

2000-08-29 **Keywords:** online auctions fraud law enforcement investigation complaints government agency industry

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cti455.htm>

### Vol #

The Internet Fraud Complaint Center, a project of the FBI and the Department of Justice, . . . [said] that online auctions are the No. 1 source of complaints about fraud on the Internet, and expects to receive more than 1,000 complaints a day starting in November when the center is fully automated. The online auction industry denies that fraud is a serious problem, and eBay says that only one of every 40,000 listings has resulted in a confirmed case of fraudulent activity. Complaints about Internet fraud can be reported to http://www.ifccbi.gov. (USA Today 29 Aug 2000)





2000-10-16 **Keywords:** online auction purchase e-commerce fraud insurance guarantee confidence NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20001016/t000098573.html >

#### Vol #

Yahoo is launching a new program to protect consumers who make purchases made on its auction and shopping sites from fraud. The initiative, which is backed by insurance from Lloyd's of London, is designed to "add another layer of confidence for consumers during the shopping season," says Brian Fitzgerald, producer for Yahoo auctions, who adds that fraudulent transactions account for less than 1% of all purchases on the Yahoo commerce site. (AP/Los Angeles Times 16 Oct 2000)

2000-11-13 **Keywords:** online auction law lawsuit judgement copyright infringement NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/2000/11/13/technology/13EBAY.html >

#### Vol #

A provision of the federal 1996 Communications Decency Act that had been written to protect Internet service providers. . . [was] extended by a California state judge in San Francisco to apply as well to eBay, the online auction company. A lawsuit against eBay charged it was liable for customer sales of bootlegged music sold through its Web site, but Judge Stuart R. Pollak rejected that contention, noting that eBay did not select the items to be sold, determine their minimum price, inspect them ... nor did it ever have them in its possession. (New York Times 13 Nov 2000)





# 1B7 Hate groups, speech

2000-02-18 **Keywords:** hate speech Web Internet censorship government law regulation restriction international

**Inter Press Service** 

Vol #

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 concluded that as long as the US First Amendment protects racist and hate-spewing sites based in that country, international efforts at control are doomed.

2000-02-24 **Keywords:** hate groups terms of service acceptable use ISP lawsuit Benton Project; USA Today

Vol #

The Jewish Anti-Defamation League protested to Yahoo for allowing several hatespeech groups on its service.





2000-10-17 **Keywords:** hate groups online identification recognizing law enforcement NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/aponline/nyregion/AP-Hate-Internet.html >

Vol #

The Anti-Defamation League, www.adl.org, has created an online guide to hate symbols, logos, and tattoos to help people become aware of warning signs of the development of "hate" groups in their communities. A police official friendly to the ADL project says, "There are new symbols out there all the time. Unless you're affiliated with these groups, these are symbols you wouldn't have any idea about." (AP/New York Times 17 Oct 2000)





# 1C1 Impersonation

2000-02-16 **Keywords:** impersonation penetration bad password guessing online chat NewsScan (reprinted with permission), CBC News < http://cbc.ca/cgi-bin/templates/NWview.cgi?/news/2000/02/15/online000215>

#### Vol #

In what was billed as the first live online interview with a sitting U.S. president, CNN's chat with President Clinton turned kinky when a computer security consultant [Christopher Petro of Lorcom Technologies, an Internet company in New York] assumed Clinton's identity and changed his response to: "Personally, I would like to see more porn on the Internet." The consultant said guessing the president's nickname was an "easy trick," and that "I hope this harmless prank has served to let CNN know that this system is insecure and needs to be overhauled before someone does actual harm to them or one of their guests." Such security flaws can easily sabotage New Media journalism if not fixed, he added. (CBC News 16 Feb 2000)





2000-06-01 **Keywords:** trademark domain name system hijacking theft forgery fraud authentication e-mail quality assurance QA

NewsScan (reprinted with permission)

Vol #

At least two Internet companies recently suffered a dot-com's worst nightmare — their domain names were reregistered without their knowledge, and all traces of their legal ownership were erased. Web.net, based in Toronto, and Bali.com of Hong Kong both have suffered crippling losses from the hijacking, which occurred last weekend. Sleuthing by Web.net's owners found that someone in Jakarta, Indonesia had sent a forged e-mail to Network Solutions, asking them to redirect all the site's e-mail and Web site information to a new location. He then requested that the registration, which had been recorded with Network Solutions in 1993, be transferred to a Toronto registrar, and asked them to switch the ownership to someone living in Hong Kong. In Bali.com's case, an investigation shows that the name now belongs to someone living in Madrid, Spain. "These are what I call A-class domain names," says Toronto Star columnist K.K. Campbell. "If the person collected 50 of these, they'd have \$5 million in assets they could afford to sit on for a little while until they're laundered and then resold." (Toronto Star 1 Jun 2000)

2000-08-17 **Keywords:** identity theft SSN social security number impersonation credit-card fraud forgery

**RISKS** 

**Vol** 21 # 02

A Professor at Central Washington University allegedly obtained the names and social security numbers of students and presented these people as the parents of imaginary children born in Massachusetts. He forged these cyberinfants' birth certificates and then applied for identification and ultimately 40 sets of credit cards. As a result of this criminal activity, the University has revised its software to exclude use of the SSNs in class listings.





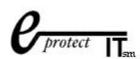
2000-08-29 **Keywords:** impersonation air traffic control radio communications spoofing RISKS, Yahoo <

http://dailynews.yahoo.com/h/ap/20000827/wl/britain\_fake\_air\_controllers\_1.html >

**Vol** 21 # 04

Joe McCauley reported in RISKS, "Britain's Civil Aviation Authority has noted various cases in which `radio hackers' have commandeered air-traffic control communications, giving false instructions or fake distress calls. The number has risen from 3 in 1988 to 18 in 1999, and 20 thus far in 2000. A case at Washington's Reagan International in April 1999 was also noted."





# 1C2 Identity theft

2000-01-16 **Keywords:** identity theft case studies prevention

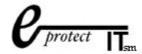
Los Angeles Times

Vol #

Caitlin Liu of the Los Angeles Times published a thorough report on identity theft on January 16 (front page). In one case, 22-year-old San Diego college student Jessica Smith had her car stolen — with her handbag inside. Although the car and bag were recovered, someone stole her identity. She nearly got fired from her new job when a background check showed that "she" had outstanding warrants for prostitution. She was unable to obtain credit, phone service or even to rent an apartment. With the help of a sympathetic police investigator, Smith was able to prove her innocence of the charges — a reversal of the usual burden under criminal law, where usually the state has to prove guilt. She obtained judicial documents explaining that her identity had been stolen; nevertheless, she has been hauled into police stations to be fingerprinted to prove that she is indeed the person authorized to carry those documents.

Image Data LLC, an identity-fraud prevention service based in Nashua, NH, commissioned a study in September 1999 that suggested that one out of five Americans or a member of their family have been victimized by identity fraud. [Readers should always be wary of statistics that report how many "members of your family" or "people you know" have particular characteristics: it is possible that a single person can be reported by multiple people. The over-counting bias increases as a function of sample size and of social relationships among the sample population.]





2000-07-13 **Keywords:** identity theft impersonation credit-card fraud legislation law proposal NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/articles/A31663-2000Jul12.html>

#### Vol #

U.S. Senators Jon Kyl (R-Ariz.) and Diane Feinstein (D-Calif.) have introduced a bill to reduce the chances of identity theft, which Feinstein says "any thief with a computer can do anonymously," because "the Internet is making it very easy." The bill would require credit-card issuers to confirm any change of address with a cardholder within ten days, and would require "fraud alerts" to be conspicuously placed on credit reports once a consumer notifies a credit bureau of identity theft. The FTC site on identity theft is www.consumer.gov/idtheft/. (Washington Post 13 Jul 2000)

2000-07-18 **Keywords:** identify theft privacy social security number SSN database disclosure Web RISKS

**Vol** 20 # 95

Given the foolish reliance of many credit-card companies and financial institutions on one's mother's maiden name as an authentication mechanism, the State of Texas has recently taken a giant step in increasing identity theft: they put birth records on the Web. Bill Tolle reported to RISKS, "Go to <

http://userdb.rootsweb.com/tx/birth/general/search.cgi > .Enter `Smith' as Surname. Leave all other fields blank. The search engine will return 35,072 names (first, last, and middle) with birth dates and the Mothers Maiden name (first, last, and middle) and Father's name (first, last, and middle)."





2000-09-25 **Keywords:** identity theft fraud government

**RISKS** 

**Vol** 21 # 07

Peter G. Neumann reported a shocking case of irresponsibility at a government service: "An AP item (seen by me on the front page of the \*Palo Alto Daily News\*, 25 Sep 2000) says that the California Department of Motor Vehicles issued over 100,000 fraudulent drivers' licenses in 1999, and typically makes little or no effort to check the validity of the 900,000 duplicate license requests it receives each year. Examples include duplicate licenses issued to people of the wrong race or the wrong gender, and in one case bogus duplicates of a particular individual's license to 18 different people. The driver's license is called a ``breeding document'' for identity thieves, leading to financial fraud, ruined credit, purchases of firearms by felons, and other misuses. DMV officials claim that implementing an on-line photo-retrieval system would cost \$3 million over the next two years. This seems like a useful system -- especially if it were used pervasively."

2000-12-12 **Keywords:** automobile drivers identity license forgery theft counterfeit break-in RISKS

**Vol** 21 # 15

In Gresham, OR, thieves broke into the state Department of Motor Vehicles office and, in less than two minutes, stole equipment for forging drivers' licenses plus computerized information about 3,215 recent holders of valid licenses. Such information and equipment is ideal for creating bogus identification documents and contributes to, among other crimes, theft of identity.





# 1D1 Organizations, cooperation

2000-01-10 **Keywords:** law enforcement network Law Net US government crime initiative

investigation criminal hackers Web vandalism international cooperation

federal state local cybercrime

AP

Vol #

In the wake of high-profile criminal attacks on e-commerce, US Attorney General Janet Reno announced her intentions to set up an information-sharing network among federal, state and local law-enforcement authorities to fight cybercrime. The "LawNet" proposal would include setting up cybercrime laboratories whose costs could be shared among participating agencies. In addition, the AG recommended a new system for speeding interstate transfers of subpoenas and warrants necessary for investigations of Internet-related crime. New York Attorney General Eliot Spitzer said, "It is perhaps not Big Brother we should be worried about, but Big Browser."

2000-01-10 **Keywords:** law enforcement cybercrime initiative proposal plan federal government NewsScan, Los Angeles Times, Edupage, EPIC Alert

Vol #

The Clinton administration proposed a national plan for fighting cybercrime. In January 2000, Attorney General Janet Reno described an information-sharing network for law enforcement and several new cybercrime labs staffed by law enforcement personnel from the federal, state and municipal levels. She proposed that law enforcement agencies have cybercrime coordinators on call. The administration plan would increase funding for academic research in INFOSEC and undergraduate scholarships by \$160M to a total of \$621M; the new federal Institute for Information Infrastructure Protection would also foster joint government-industry task forces for security research.





2000-01-17 **Keywords:** government law enforcement police Internet cybercrime

Times of London

Vol #

The British Home Secretary, Jack Straw, announced plans for a national computer-crime squad. He authorized the National Criminal Intelligence Service (NCIS) to develop a specialized team to attack Internet crimes such as fraud, money laundering, pornography, illegal gambling and pedophile rings. The squad would collaborate with other agencies such as the taxation department (Inland Revenue), domestic security intelligence (MI5) and the international surveillance center (GCHQ).

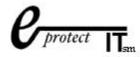
2000-02-17 **Keywords:** law enforcement international cooperation networking sharing information Europe

Daily Telegraph (London)

Vol #

The European Commission began a process for improving the battle against cybercrime. The Commission was considering setting up a special school for law enforcement to learn more about fighting cyberspace crime; another idea was increased involvement by Interpol in criminal investigations involving computers and networks.





2000-02-18 **Keywords:** law enforcement fraud cyberspace securities funding

Newsbytes

Vol #

The Securities and Exchange Commission (SEC) announced that it was hiring about 100 new officials to fight cyberspace fraud, of which 60 will police the Web. There were already 250 workers scanning the Web full time, said the Chairman, Arthur Levitt in mid-February 2000. He cited a "frightening" recent case in which a criminal hacker inserted false news of a merger on a company Web site. Stock manipulations include rumor-mongering to drive up the price of stock already held and also to drive down the price of stocks already sold on the futures market at a higher price than the desired target.

2000-03-24 **Keywords:** fraud law enforcement government agency investigation prosecution international cooperation

NewsScan (reprinted with permission)

Vol #

The U.S. Federal Trade Commission . . . [said] it's been working with other international organizations in an unprecedented global effort to crack down on fraudulent, get-rich-quick schemes that are promoted through the Internet. The sweep, which began in February, involved 28 countries and targeted 1,600 suspect Web sites. Typical scams included pyramid schemes, unrealistic investment opportunities and easy-money come-ons. Domestically, the FTC has enlisted the help of the Postal Service and the Securities and Exchange Commission enforcement units to assist in monitoring online fraud. FTC officials say the sites have now been warned that they must change their claims or it will attempt to have them shut down. "We're going to run them off the Web and where appropriate, put them in jail," says Drew Edmondson, attorney general of Oklahoma. (Financial Times 24 Mar 2000)





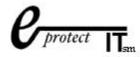
2000-05-08 **Keywords:** fraud law enforcement consumer report investigation prosecution Web Internet

NewsScan (reprinted with permission)

Vol #

The U.S. Department of Justice and the Federal Bureau of Investigation are collaborating on the creation of an Internet Fraud Complaint Center, which will give consumers and businesses a one-stop shop for reporting incidents in which a computer was used for criminal activity, such as fraudulent claims made over a Web site, via e-mail, or in chat rooms. It will not cover crime in which computers were the target, such as the distributed denial of service attacks that crippled some major businesses' computers recently. Those problems should be addressed by the National Infrastructure Protection Center. (TechWeb 8 May 2000)





2000-05-14 **Keywords:** computer crime international cooperation jurisdiction laws legislation regulations investigations treaty standards

NewsScan (reprinted with permission), San Jose Mercury News

- < http://www.sjmercury.com/svtech/news/breaking/merc/docs/011053.htm> , Los Angeles Times
- < http://www.latimes.com/business/20000518/t000046914.html>

#### Vol #

With the "Love Bug" virus providing a recent reminder of the problem of cybercrime and other kinds of mischief on the Internet, leaders from the Group of Eight countries . . . [met] to see what can be done, and the 41-nation Council of Europe is working with the U.S., Canada, Japan and South America to draft a treaty to standardize laws against Internet crime. Jonathan Fornici of the Internet security consulting firm AtomicTangerine says that governments need to write laws that make the punishment clear, because the way things are now, people know security violations are wrong -- "but what's the repercussion?" In the Love Bug case, investigators in the Philippines delayed a raid for several days until prosecutors found a law that might apply. (AP/San Jose Mercury News 14 May 2000)

[When] Envoys from the world's leading industrialized nations and private business met . . . in Paris to discuss cooperation in fighting Internet-based crime, [there were] . . . widespread differences in national approaches [that] could stymie efforts. At the heart of those differences is the degree to which governments are willing to monitor the Net for illegal behavior, which inevitably occurs at the expense of citizens' privacy. In addition, e-commerce businesses tend to discourage more government involvement, which they view as a menace to both economic growth and individual liberty. On April 27, the Council of Europe published a draft treaty proposing uniform international law enforcement standards in cyberspace, including the requirement that all messages and content sent via the Internet be stored for three months before deleting. That proposal has met with mixed reactions among both governments and industry representatives. The U.S., which held observer status during the drafting, . . . [did not endorse] that proposal. (Los Angeles Times 18 May 2000)





2000-07-19 **Keywords:** civil liberties investigation monitoring interception privacy law enforcement government program encryption keys passwords

NewsScan (reprinted with permission), San Jose Mercury News

- < http://www.sjmercury.com/svtech/news/breaking/internet/docs/374641.htm>, New York Times
- < http://www.nytimes.com/library/tech/00/07/biztech/articles/19britain.html> , USA Today

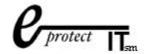
#### Vol #

The British government . . . [said] its plans to allow security services to monitor Internet traffic . . . [would] not create an overly intrusive cyberspace spy agency, but civil liberties groups argue the Regulation of Investigatory Powers (RIP) bill would give police free rein to snoop on the Internet and could result in people being jailed for forgetting their passwords. The bill would require citizens to reveal encryption keys to the police or face a two-year jail term. "The police have to prove the encryption key was deliberately withheld," says a Home Office spokesman. "We're not talking about people going to prison for forgetting passwords... Interception of communications is only used on the authorization of the Home Secretary himself. And it's only used in defense of national security or on suspicion of serious crime, like narcotics smuggling or terrorism." (Reuters/San Jose Mercury News 26 May 2000)

[In July,] UUNet and Nokia . . . [participated] in a last-ditch effort to derail the controversial U.K. Regulation of Investigatory Powers Bill, which would allow law enforcement officials to require ISPs to intercept e-mail messages and other data on their systems. Individuals or companies sending encrypted data could be required to provide it in plan text or surrender a software encryption key to decode the message. UUNet called the legislation, to be debated today in the House of Lords, "fundamentally flawed" and "draconian," and added, "It would be tragic if by imposing a new requirement on ISPs, the U.K. were to make itself uncompetitive in the provision of Internet services. We would ask the government to step back and rethink the whole bill." Meanwhile, Nokia is the first company to voice concern over the legislation based on its impact on future wireless services. (Financial Times 12 Jul 2000)

[Also in July,] . . . . A government official argued that "the powers in the bill are necessary and proportionate to the threat posed by 21st century criminals, no more, no less." The bill has angered civil libertarians, and a spokesperson for Amnesty International in London said: "What this does is contravene a large number of fundamental rights in the European convention on human rights and other international standards, which include the right to privacy, the right to liberty, the right to freedom of expression, and the right to freedom of association." (New York





Times 19 Jul 2000)

[At the end of July, the British] Parliament . . . passed legislation that will allow law enforcement authorities to demand records of Internet traffic for scrutiny by MI5, the country's domestic intelligence agency. The rationale for the new law is that it's necessary to counter the increasing technological sophistication of organized criminal efforts; however, one Labor Party dissenter said that certain provisions of the bill "are born of complacency, are unsatisfactory, and have little regard for the protection of privacy and commercial confidences." (AP/USA Today 28 Jul 2000)

2000-09-26 Keywords: fraud prevention investigation law enforcement international commerce

organization alliance consortium teaching support resources

clearinghouse best practices

NewsScan (reprinted with permission), E-Commerce Times < http://www.ecommercetimes.com/news/articles2000/000926-3.shtml>

Vol #

A group of leading U.S. e-commerce merchants and payment processing companies have formed an industry coalition to reduce online fraud. The Worldwide E-Commerce Fraud Prevention Network, which includes American Express, Buy.com and Expedia, will serve as a clearinghouse for information on best fraud prevention practices and current fraud prevention trends, as well as security seminars, law enforcement resources and security software vendors. One of the main concerns for members is that online merchants are often held liable for the cost of goods purchased with stolen credit cards. "More than 41% of the merchants we canvassed didn't know that they -- not the credit card companies -- are liable for fraud," says one security software firm executive. "Online credit card fraud is projected to cost merchants US\$9 billion annually by next year." (E-Commerce Times 26 Sep 2000)





# 1D2 Technology

2000-02-03 **Keywords:** wiretapping Internet standards law enforcement police government regulations opposition debate discussion decision ruling

POLITECH, Wired < http://www.wired.com/news/print/0,1294,34055,00.html >

Vol #

The IETF rejected proposals for including support for wiretapping in Internet standards.

2000-02-04 **Keywords:** technology criminal hacker evidence encryption legal law judge ruling trial case

New York Times < http://www.nytimes.com/library/tech/00/01/cyber/cyberlaw/28law.html >

Vol #

During the Mitnick trial, defense lawyers were given the contents of hard disk drives seized from laptop computers belonging to the defendant — save for the roughly 1 Gb of encrypted data for which Mitnick refused to reveal the encryption key(s), as he was fully entitled to do under the prerogatives of the Fifth Amendment of the US Constitution forbidding self-incrimination. On May 20, 1998, the federal judge, Mariana R. Pfaelzer of the Los Angeles district, agreed with prosecutors that they could keep the encrypted data from the defense team. Some legal experts disagreed with the ruling, saying that in the absence of evidence to the contrary, the encrypted data should not have been sequestered by the government side. The problem would recur, they said, as disk encryption became more widespread.





2000-04-30 **Keywords:** e-mail interception monitoring government law enforcement police Internet

Sunday Times < http://www.sunday-times.co.uk/news/pages/sti/2000/04/30/stinwenws01034.html >

#### Vol #

Reports in Britain detailed government plans to build a monitoring center capable of scanning all inbound and outbound e-mail and mobile phone calls in the UK. Plans included requirements for permanent linkages between the center and ISPs. Although a warrant would be required for examination of communications to individuals, approval for interception of corporate e-mail would be easier to obtain. The proposal for the GTAC (Government Technical Assistance Centre) raised a storm of protest from civil liberties advocates.





2000-07-11 **Keywords:** Internet service provider ISP surveillance wiretap interception monitoring law enforcement privacy protests e-mail investigation sniffer

NewsScan (reprinted with permission), Wall Street Journal

- < http://interactive.wsj.com/articles/SB963264584706292829.htm> , Washington Post
- < http://www.washingtonpost.com/wp-dyn/articles/A15206-2000Jul20.html> , Washington Post

#### Vol #

The Federal Bureau of Investigation is using a superfast e-mail-surveillance software system called Carnivore, so named because it can quickly ferret out "the meat" among a vast quantity of data in search of criminal or terrorist content. FBI investigators say the Internet wiretapping system has been used in fewer than 100 criminal cases since its launch last year, but privacy advocates say its deployment gives government, at least theoretically, the ability to eavesdrop on all customers' digital communications, from e-mail to online banking to Web surfing. The FBI defends Carnivore as more precise than the primitive Internet wiretap systems used in the past, and credits it with the ability to target the digital traffic of just one user amidst a stream of millions of other messages. "This is just a very specialized sniffer," says Marcus Thomas, head of the FBI's Cyber Technology Section, but Republican Congressman Bob Barr (R-Ga.) counters, "Once the software is applied to the ISP, there's no check on the system. If there's one word I would use to describe this, it would be 'frightening.'" (Wall Street Journal 11 Jul 2000)

The Republican Congressional leadership . . . [opposed] Clinton Administration plans to use its "Carnivore" software system to monitor a criminal suspect's e-mail messages as they pass through an Internet service provider. The FBI says this system is not intended to extend the government's surveillance capabilities, but merely to update their methods to cope with changing technology, but House Majority Leader Dick Armey (R-Tex.) says: "Nobody can dispute the fact that this is not legal within the context of any current wiretap law... We have a Congress that is anxious to work with [the Administration] ... but in effect they have said: 'We're going to go on our own and not wait for technology or the Congress to catch up with our desires for cyber-snooping.' That's a dangerous thing for us to allow to go along unchecked." (Washington Post 21 Jul 2000)

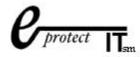
In testimony before a House Judiciary subcommittee, FBI official Donald M. Kerr strongly defended the agency's use of the "Carnivore" system, which effectively places a wiretap on the Internet and allows law enforcement officials to identify the origin and destination of all e-mail messages related to a person under suspicion of a crime. The reaction of Rep. Spencer Bachus (R-Ala.) was skeptical: "The potential for abuse here is tremendous. What you're saying is 'Trust us.'" But Kerr insisted that





Carnivore was an essential tool for fighting crime: "Criminals use computers to send child pornography to each other using anonymous, encrypted communications. Hackers break into financial service companies' systems and steal customers' home addresses and credit-card numbers, criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world, and terrorist bombers plan their strikes using the Internet." Civil liberties groups have been consistently critical of the FBI's support of Carnivore. (Washington Post 25 Jul 2000)





2000-08-03 **Keywords:** privacy surveillance wiretapping interception law enforcement investigation civil liberties e-mail

NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/articles/A25897-2000Aug2.html> , San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/021106.htm>

#### Vol #

U.S. District Judge James Robertson . . . ordered the Justice Department to expedite its review of requests by the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC) for background materials on "Carnivore," a software tool developed to help the FBI carry out court-approved monitoring of suspected criminal activity on the Internet. An attorney for EPIC says, "The fact that the court is going to supervise the processing of the material is very good news. If left to their own devices, it's likely the FBI would tend to drag its feet on this, and now I think that's less likely. . . . It's going to be very difficult to have a meaningful debate about the legal issues Carnivore raises if we don't really know what Carnivore is." (Washington Post 3 Aug 2000)

Attorney General Janet Reno . . . asked the Justice Department to select a U.S. university to do an objective review of the FBI's "Carnivore" e-mail surveillance system, which scans Internet data packets as they travel to and from a criminal suspect. Civil liberties groups have been demanding that they be given all the information needed to understand how the system operates. They are not happy with Reno's decision. ACLU executive Barry Steinhardt says a university-conducted review will not be "truly independent" and adds: "The fox doesn't get to choose who guards the henhouse." (AP/USA Today 10 Aug 2000)





2000-08-11 **Keywords:** surveillance law enforcement international jurisdiction wiretaps access foreign control national security

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB965952625894025409.htm>

#### Vol #

[In July,] The Federal Bureau of Investigation . . . voiced national security concerns regarding Nippon Telegraph & Telephone's planned acquisition of U.S. Internet service provider Verio. The agency has complained in recent years that its ability to maintain surveillance over U.S. telecommunications networks could be compromised by foreign ownership deals, and this latest statement indicates those concerns are now moving into the Internet arena. FBI fears are focused on the possibility of foreign companies moving network operations offshore, which could constrict the agency's ability to physically access Internet gear to conduct wiretaps. Experts say the deal probably will be approved, but have expressed concern about the precedent it will set: "I'm confident it can be worked out, but the willingness of the government to take [its inquiry] this far and get assurances they probably don't need is not a good idea," says a lawyer specializing in telecommunications and Internet regulatory matters. (Wall Street Journal 6 Jul 2000)

[In August,] The Federal Bureau of Investigation has negotiated an agreement with Nippon Telegraph & Telephone that sets conditions for the Japanese firm's \$5.5 billion purchase of U.S. Internet service provider Verio. The agreement provides a number of safeguards to protect U.S. law-enforcement investigations, including a ban on Japanese government involvement in Verio's day-to-day activities (the government still owns a sizeable stake in NTT). Critics contend that the FBI overstepped its authority in laying down conditions of the sale: "If there's a lesson learned, it's get the FBI out of these transactions, because they're extracting concessions that may be beyond what the law requires," says Albert Gidari, a Seattle lawyer who specializes in regulatory issues. (Wall Street Journal 11 Aug 2000)





2000-08-17 **Keywords:** law enforcement surveillance civil liberties monitoring surveillance interception Internet service provider ISP

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/021106.htm>

Vol #

Civil libertarians. . . [were] unhappy with the Justice Department's response to a Freedom of Information request that it release for scrutiny all 3,000 pages of documents describing the FBI's "Carnivore" e-mail surveillance system. Their complaint is that the proposed schedule for releasing the documents "could stretch on for many months or even years." The government says that the deliberate pace is required by the fact that commercial entities that contributed to Carnivore as government contractors need the opportunity to review and express an opinion on the disclosure of information they provided. (AP/San Jose Mercury News 17 Aug 200)

2000-08-26 **Keywords:** fingerprint registration number keyspace rollover police law enforcement technology identity confusion duplicates synonyms collisions

**RISKS** 

**Vol** 21 # 02

In New York State, the fingerprint ID registration field is only 7 digits long, producing a maximum of 10,000,000 values -- but the population is currently 18M and there are many historical records. The decision to begin re-using the IDs alarmed security specialists despite assurances that no one would be misidentified.





2000-09-07 **Keywords:** law enforcement surveillance civil liberties monitoring surveillance interception Internet service provider ISP

NewsScan (reprinted with permission)

Vol #

Internet pioneer Vinton Cerf told a Senate committee . . . [on 6 Sep] that he is satisfied that the FBI's use of the Carnivore e-mail monitoring system won't violate the privacy of Internet users. Cerf added that the efforts by some civil liberties groups to force the FBI to reveal Carnivore's source code are misguided. "I don't want you to misunderstand that I think this is all great," he said, agreeing that the potential for abuse is there. "I don't believe what the FBI has done is abusive. Used in the fashion described, it is very constrained in its data capture." Cerf's reservations about disclosing the source code were echoed by Judiciary Committee chairman Orrin Hatch: "ISP geeks may be less familiar with the penalties and restraints than the gentlemen from the FBI." The Justice Department has agreed to an independent review of Carnivore by a panel of academic experts it will select, but some top security experts say the conditions set for the review are tyrannical: "Independent has a new meaning in DOJ parlance," said Peter G. Neumann, principal scientist at SRI International Computer Science Laboratory. "Independent means total censorship, total control over content." (Wall Street Journal 7 Sep 2000)





2000-09-19 **Keywords:** Internet service provider ISP surveillance wiretap interception

monitoring law enforcement privacy protests e-mail investigation sniffer

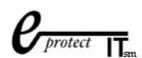
alternative

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/054462.htm>

Vol #

NetICE, a software security company, has developed a free and open software product called "Altivore" as "alternative to Carnivore," the e-mail surveillance system favored by the FBI but criticized by privacy advocates. The company's chief technology officer said: "We wrote Altivore to correspond exactly to what the FBI says what Carnivore does... We founded this company in order to protect peoples' privacy. By showing the source code for Altivore, we're narrowing the debate to the true issues.'' Altivore can be downloaded free from the company's Web site. (AP/San Jose Mercury News 19 Sep 2000)





2000-10-05 **Keywords:** records justice judge deletion archives discard destroy invalid inadmissible evidence e-mail communications permanent

NewsScan (reprinted with permission), New York Times < http://.nytimes.partners.com/2000/10/05/technology/06CYBERLAW.html >

#### Vol #

District Court Judge James Rosenbaum has published an article called "In Defense of the DELETE Key," in which he bemoans the eternal nature of computer communications and reminisces fondly about pre-computer days when people casually spoke "off the record": "At this earlier time, two people could easily say something -- even, perhaps, something politically incorrect -- simply between themselves. They might even have exchanged nasty notes between themselves. And when they had moved past this tacky, but probably innocent moment, it was truly gone." Today, however, "an idle thought jotted onto a calendar, a tasteless joke passed to a once-trusted friend, a suggestive invitation directed at an uninterested recipient, if done electronically, will last forever. Years later, it can subject its author to liability." Rosenbaum proposes a "cyber statute of limitations" -- perhaps six months for an isolated e-mail message -- after which "deleted" documents would be legally consigned to the electronic rubbish heap and become inadmissible as evidence of possible wrongdoing. He makes an exception for recovered "deleted" messages from someone who has exhibited a pattern of egregious behavior or communications. The article was published in the Summer issue of The Green Bag, a literary law journal. (New York Times 5 Oct 2000)





2000-10-06 **Keywords:** fraud lawsuit prosecution criminal fraud pornography telephone cramming theft tracking software trace IP address law enforcement

NewsScan (reprinted with permission)

Vol #

The Federal Trade Commission filed a complaint in federal court . . . [Oct 2] alleging that Verity International, which is registered in Dublin and is no relation to the California software company Verity Inc., improperly charged thousands of U.S. Internet users for long-distance phone calls. The porn customers were told they were being charged to view sex videos over a phone line to Madagascar at a rate of \$3.99 a minute, but the FTC determined that the calls actually terminated in the U.K. and should have cost only eight cents a minute. Verity planned to pocket the difference. The scope of the scam was huge -- in a single week in September, some 67,000 U.S. households received bills from Verity, with an average overcharge of \$222 (although some overcharges topped \$4,000). Interestingly, the agency used an off-the-shelf software program called NeoTrace to locate the alleged perpetrators. According to NeoTrace's manufacturer, NetWorx, the software is used by the FBI, the U.S. Customs Service, NATO, the Royal Canadian Mounted Police and Interpol to trace the geographic origin of Internet traffic. (Wall Street Journal 6 Oct 2000)





2000-12-07 **Keywords:** law enforcement investigation wiretap e-mail address law ruling debate regulations

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB976146889727650215.htm >

#### Vol #

Law enforcement officials have long held that a 1986 law allowing police to record phone numbers by someone tied to a criminal investigation permits them to secretly copy e-mail addresses in messages sent to people involved in criminal probes, but a newly disclosed e-mail message suggests there is internal dissension over the legality of such "pen traps": "We have agents that would like to use a pen for e-mail, but our [chief division counsel] thinks that we can only use a pen to get the telephone number dialed by the modem," one agent wrote in the Feb. 14 e-mail. "I don't think we in the field have a grasp of how the existing telecommunications laws apply to computer communications." Highlighting the depth of confusion over the issue within lawenforcement circles, the agent noted that this legal opinion came from the FBI's National Infrastructure Protection Center, which includes the bureau's top computercrime experts in Washington. The uncertainty brings into question the legality of using Carnivore, the FBI's e-mail "sniffing" software, which has been justified under the 1986 law that covers any device that "records or decodes electronic or other impulses, which identify the numbers dialed or otherwise transmitted" and that is attached to a telephone line. "Carnivore is not attached to a telephone line and does not obtain a number dialed," says Philip L. Gordon, a lawyer with the Privacy Foundation, who notes that privacy protections for e-mail addresses should be greater than those for phone numbers. "They're clearly different." (Wall Street Journal 7 Dec 2000)





# 1D3 Litigation, legal rulings, judgements

2000-01-14 **Keywords:** privacy law evidence wiretapping

NewsScan, New York Times <

http://www.nytimes.com/library/tech/00/01/cyber/cyberlaw/14law.html >

Vol #

In Spokane County (Washington) Superior Court, the defense in a rape and child porn trial argued that the state's privacy laws precluded law-enforcement use of captured e-mail and chat-room messages. However, Superior Court Judge Kathleen M. O'Connor denied the motion, stating that the law does not specifically include computers as a protected medium.

2000-02-18 **Keywords:** wiretapping telecommunication criminal hacking phreaking

The Times (London)

Vol #

In England, the House of Lords ruled in favor of Stephen Alan Morgans, who appealed a conviction based in part on log files printed out from a device placed on the defendant's telephone line. The printouts showed that Mr Morgans had accessed phone company computers and fraudulently obtained phone services. Unfortunately, police had failed to obtain a warrant from the office of the Secretary of State. The Lords threw out the conviction on the grounds that the intercepts were illegal.





2000-07-07 **Keywords:** law enforcement court case judgement entrapment investigation Internet e-mail

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/library/tech/00/07/cyber/cyberlaw/07law.html>

#### Vol #

A majority of a three-judge U.S. appellate court panel . . . ruled against the use of the Internet to entrap an individual into committing sex offenses. After being divorced by his wife because he could not control his compulsion to cross-dress, the individual in question began to use the Internet to search for a woman who would accommodate his sexual tastes. He entered into correspondence with someone called Sharon, who tuned out to be an undercover police investigator, who suggested the idea of having sex acts with her children. The man was arrested when he showed up at a meeting place to carry out the plan. The court ruled: "Prior to his unfortunate encounter with Sharon, [the man charged for attempting to have sex with minors] was on a quest for an adult relationship with a woman who would understand and accept his proclivities, which did not include sex with children. There is surely enough real crime in our society that it is unnecessary for our law enforcement officials to spend months luring an obviously lonely and confused individual to cross the line between fantasy and criminality." (New York Times 7 Jul 2000)





# 1D4 Government funding

2000-02-07 **Keywords:** budget proposal administration wiretapping law enforcement military telco telephone company

Wired < http://www.wired.com/news/politics/0,1283,34164,00.html > , NewsScan, Washington Post < http://www.washingtonpost.com/wp-dyn/articles/A32193-2000Aug15.html>

#### Vol #

In February, the Clinton administration proposed a \$1.84T budget fiscal 2001 that would include major increases in spending on law enforcement capabilities such as wiretapping. The government would reimburse telcos to the tune of \$240M (up from \$15M) under the controversial CALEA (Communications Assistance to Law Enforcement Act) for rewiring their networks to make wiretapping easier.

[However, in August (wrote the NewsScan editors), A three-judge panel of the U.S. Court of Appeals for the District of Columbia . . . ruled that the Federal Communication Commission's attempts to implement a 1994 electronic wiretap law have been too accommodating to law enforcement agencies and not sufficiently protective of the right of citizens to individual privacy or of the financial requirements of companies. The wiretap law (the Communications Assistance for Law Enforcement, or CALEA) was passed by Congress because the FBI had insisted it was losing ground against criminals because wireless phone companies were not designing wiretapping capabilities into their networks. An executive of the Center for Democracy and Technology, which had opposed the FBI's request to Congress, . . . [said] the appellate court's decision means that "government cannot get its hands on what it's not authorized to get just by promising it won't read what it's not supposed to read." (Washington Post 16 Aug 2000)





# Quality assurance failures (general)

2000-01-03 **Keywords:** Y2K quality assurance success

Edupage, Washington Post, Wall Street Journal

Vol #

On the whole, the IT world was delighted to see that Y2K fixes worked. As the New Year opened, few major problems were reported worldwide. Skeptics began murmuring that the entire exercise had been futile and that warnings of Y2K difficulties had been exaggerated. [Presumably these same people were prepared to burn fire stations for their annoying insistence on fire prevention techniques in the absence of worldwide conflagration.]

2000-01-04 **Keywords:** Web site quality control QA assurance checking erotic inappropriate books videos advertising merchandising

NewsScan, Los Angeles Times < http://www.latimes.com/business/20000104/t0000010000.html >

Vol #

Wal-Mart Stores, Inc. discovered guidebooks to erotic videos being advertised on its new Web site. A spokeswoman apologized for the failure of quality control in checking a third-party supplier's lists and promised to expunge references to "The Best of Gay Adult Videos" and "The Couple's Guide to the Best Erotic Videos."





2000-01-09 **Keywords:** Y2K failures screen shots Web sites archive

**RISKS** 

**Vol** 20 # 74

The site < http://y2kmistakes.com > published an extensive list of screen shots from Web sites with Y2K problems.

2000-01-19 **Keywords:** DNS WHOIS quality assurance QA

NewsScan, Wired < http://www.wired.com/news/technology/0,1282,33753,00.html >

Vol #

BulkRegister, a recently approved Internet domain name registrar, apparently has goofed. It allegedly sold several domain names to customers and then released them for sale again a day or two later, at which point they were resold by other registrars. The more recent buyers are the ones that show up in the master Whois.com database, which controls who can set up a site using that URL. "We are not allowed physically to access these domains," says one frustrated BulkRegister purchaser. "We couldn't put up a site, even though BulkRegister claims we own them." Some of the names sold twice include kids.com, welcome.com and eDiscount.com. (Wired.com 19 Jan 2000)

2000-01-23 **Keywords:** QA quality assurance e-mail

**RISKS** 

**Vol** 20 # 75

E-mail program MS-Outlook automatically interprets the string "begin" followed by two spaces as an instruction to interpret all remaining text as an attachment (and thus rendering it invisible). There is no option with which to turn this helpful feature off.





2000-01-26 **Keywords:** privacy violations error quality assurance Web embarrassing

NewsScan, New York Times < http://www.nytimes.com/aponline/f/AP-Internet-Privacy.html > **Vol** #

Two companies escaped prosecution by settling with the New York State Attorney General in January. Both companies (Chase Manhattan Bank and InfoBeat) had erroneously revealed private customer data on their Web sites due to bad programming. The Bank compromised data for 18 M credit-card and mortgage holders; the Internet company gave customer e-mail addresses to advertisers by mistake.





2000-02-07 **Keywords:** design boundary conditions quality assurance QA stress testing overload denial of service

 $News Scan \ (reprinted \ with \ permission) \ St \ Petersburg \ Times \ (FL) < http://www.sptimes.com/> \ , \\ MSNBC < http://www.msnbc.com/news/365664.asp>$ 

#### Vol #

A new Web site promising to give away \$10,000 a day in scholarship money to the lucky visitor who wins the luck of the draw [was launched on 3 Feb]. The Cambridge, Mass.-based company FreeScholarships.com is financing its giveaways through marketing groups and advertisers eager to access the teenage and 20-something population. The money is available for college, graduate school, or private school for children, and winners need only be U.S. citizens over the age of 13. Applicants must divulge some amount of demographic data to qualify, and winners are chosen by computer-generated random drawing. The odds of winning depend on how many log on. And for those who don't win? FreeScholarships.com also offers tips on financial aid. (AP/St. Petersburg Times 3 Feb 2000)

FreeScholarships.com found out that handing out money can be harder than it looks sometimes. On [the first day of operation] the site was overwhelmed with visitors trying to register for the tuition giveaway, causing the servers to crash. Technicians were still working on the problem [the next day]. The site, described by its founder as "a low-energy path for people to get a shot at helping them pay for school," plans to give away \$10,000 a day to students seeking funds for college, graduate programs, private or parochial school. Additional drawings will give away \$25,000 every month and \$50,000 each quarter. (MSNBC 4 Feb 2000)

[This case illustrates the critical importance of appropriate design and of stress testing as part of quality assurance.]





2000-02-15 **Keywords:** quality assurance QA bug design

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/2000215/t000014636>

#### Vol #

A computer glitch at the Internal Revenue Service is responsible for rejecting about 40,000 electronically filed returns before the error was discovered and fixed last week. An "error reject code" was triggered when taxpayers sent returns that included a child-care credit or dependent-care benefits. The IRS suggests that the rejected returns be refiled. Congressional guidelines call for 80% of all returns to be filed electronically by 2007. (Los Angeles Times 15 Feb 2000)

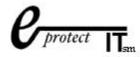
2000-02-16 Keywords: quality assurance, QA bug government

NewsScan (reprinted with permission)

#### Vol #

Tax preparer H&R Block, which [expected] to use the Internet this season to file the tax returns of 650,000 of its customers, . . . temporarily discontinue[d] online filings until it [determined] how information from a small group of returns was commingled (a mix-up that apparently affected 50 or fewer of a total of 300,000). The company expects to be able to have the problem solved by next week. (AP/USA Today 16 Feb 2000)





2000-02-17 **Keywords:** information warfare Trojan software foreign contractor

AP, Washington Post

Vol #

According to a Washington post article by David Ignatius, the US State Department had its shorts in a knot because they had just realized that a software package called the Mission Performance Plan running on embassy computers around the world was written by programmers from the former Soviet Union. On 2000-02-02, the Department of State sent an urgent cable to 170 embassies ordering them to remove the package by the 7th while security specialists examine the code for trap doors, logic bombs and other cybernasties. [Comment by MK: this incident reinforces the view that the trustability of software writers is even more important than quality assurance where security is concerned. As many commentators have noted, it may be impossible in practice to apply adequate quality assurance to untrusted code. I have frequently urged QA specialists to ensure that they use code-coverage logging to ensure that every line of code is actually executed during the SQA process; however, even total coverage does not necessarily mean that a program is guaranteed safe, since variable sequence of execution could result in different outcomes for the same subroutines because of data dependencies.]

2000-02-20 **Keywords:** QA quality assurance browser patch wrong message

RISKS

**Vol** 20 # 80

A patch for a security hole in Microsoft's Internet Explorer that would allow a server with an exact filename to retrieve that file without permission from a client's hard disk itself contained a quality assurance flaw. If one attempted to install the patch on IE 4.01 with SP1 (Service Pack 1), the installer stated that the patch was not needed -- when in fact it was needed.





2000-02-21 **Keywords:** source code untrusted authors espionage

**RISKS** 

**Vol** 20 # 81

According to a 17 Feb 2000 AP item (18 Feb 2000 article in \*The Washington Post\* by David Ignatius, the US State Department has its shorts in a knot because they have just realized that a software package called the Mission Performance Plan that is running on embassy computers around the world was written by programmers from the former Soviet Union. On 2 Feb 2000, the Department of State sent an urgent cable to 170 embassies ordering them to remove the package by the 7th while security specialists examine the code for trap doors, logic bombs and other cybernasties.

[Comment by MK: this incident reinforces the view that the trustability of software writers is even more important than quality assurance where security is concerned. As many commentators have noted, it may be impossible in practice to apply adequate quality assurance to untrusted code. I have frequently urged QA specialists to ensure that they use code-coverage logging to ensure that every line of code is actually executed during the SQA process; however, even total coverage does not necessarily mean that a program is guaranteed safe, since variable sequence of execution could result in different outcomes for the same subroutines because of data dependencies.]





2000-02-23 **Keywords:** QA quality assurance operating system performance software feature bloat RISKS

**Vol** 20 # 82

RA Downes of Radsoft Laboratories published a blistering denunciation of Microsoft's continuing pattern of making its operating systems less and less efficient. Windows 2000 is even slower than Windows NT, requiring massive upgrades in processor speed, disk space and RAM to achieve equivalent throughput — and this without significant improvements in functionality, according to Downes. Current estimates of error rates at Microsoft are 4 bugs/KLoC (1024 lines of code) — and Windows 2000 is estimated to have around 60M lines of code (implying perhaps 60,000 unidentified errors).

2000-02-28 **Keywords:** quality assurance glitch bug QA broadcast channel pornography Reuters

Vol #

Canadian purveyor of professional wrestling to theaters across Canada mixed up the feed and piped in graphic pornography at the end of a WWF Entertainment show, just as families were leaving. Apparently the action was even tougher than in the ring; "It was very graphic," said Colleen Allen to a Vancouver Province reporter. "My 11-year-old was devastated. . . . Little girls were coming out crying." The company apologized and said they were rewiring their entire switching facility. [Rewiring the facility??]





2000-03-01 **Keywords:** QA quality assurance testing critical systems

**RISKS** 

**Vol** 20 # 84

Peter Ladkin of the University of Bielefeld (Germany) analyzed a report on the Wide Area Augmentation System, an adjunct to the Geographical Positioning System that should permit identification of airliners to within 3 meters (instead of today's 100 m) over the continental USA. However, one of the requirements struck experts as grounds for concern: "The probability that a pilot would \*not\* get a positive warning when WAAS guidance is erroneous for longer than 6.2 seconds must be less than 1 in 10exp7 (units - I presume approaches). This evaluates to one in 47.5 years, apparently. \*AvWeek\* points out what most safety-critical-system professionals know and others can figure out in a second or two, that confidence to this level can only be achieved by analysis and not by testing."

2000-03-03 **Keywords:** quality assurance QA software bug incompatibility denial of service NewsScan (reprinted with permission)

#### Vol #

National Discount Brokers, and online brokerage, says the outages it experienced recently were the result of "hacker-like" attacks by an unnamed Web software maker. The company had originally said its problems "had the earmarks of a hacker attack." Apparently, the periodic disruptions were the result of software incompatibility with products made by the outside company that resulted in denial-of-service-type outages. NDB says it's considering whether to pursue "appropriate judicial relief" through legal action against the company. The outages meant that NDB customers had to wait an average of 43.9 seconds to reach its site, twice as slow as the next slowest online trading site, and prevented 200,000 customers from placing stock orders online, although they could still relay orders over the phone. (Reuters/TechWeb 3 Mar 2000)





2000-03-13 **Keywords:** user interface design error judgement QA quality assurance technical support data loss error message

**RISKS** 

**Vol** 20 # 84

Dick Karpinski noted in RISKS that some voice-mail systems require the user to press the pound (#) key to save a voice-mail message. Most users assume that hanging up saves the message. Karpinksi correctly noted in an exasperated letter to a manager at Lucent Technologies, "The problem is not even that such messages are unceremoniously dumped. The problem is that the message is lost AND NO ERROR IS INDICATED. A guy can go for months telling people he DID return their voice mail while they tell him they never got it. It wouldn't take a big change to fix the problem, but all the experts chalk up the failures to inadequate training. I chalk it up to a BROKEN user interface that allows slightly forgetful users to go on making mistakes for a long time. This makes the whole organization seem stupid or irresponsible. It may die the death of a thousand cuts. This is not a trivial matter. They are your customers and they deserve better. "





2000-03-21 **Keywords:** vulnerability e-commerce passwords

RISKS; < http://cs.nyu.edu/rubin/passport.html >

**Vol** 20 # 85

Avi Rubin and Dave Kormann published a paper about security holes in Microsoft's Passport protocol; their abstract follows verbatim: Passport is a protocol that enables users to sign onto many different merchants' web pages by authenticating themselves only once to a common server. This is important because users tend to pick poor (guessable) user names and passwords and to repeat them at different sites. Passport is notable as it is being very widely deployed by Microsoft. At the time of this writing [March 2000], Passport boasts 40 million consumers and more than 400 authentications per second on average. We examine the Passport single signon protocol, and identify several risks and attacks. We discuss a flaw that we discovered in the interaction of Passport and Netscape browsers that leaves a user logged in while informing him that he has successfully logged out. Finally, we suggest several areas of improvement.

2000-04-06 **Keywords:** QA quality assurance telephone failure

**RISKS** 

**Vol** 20 #

The Australian Telstra company announced on 2000-04-06 that a software failure in its switches was preventing 76,000 subscribers from receiving incoming calls; outbound calls were functioning.





2000-04-18 **Keywords:** QA quality assurance applet

**RISKS** 

Vol 20 #

Microsoft's Explorapedia v 1.0 shows the Earth rotating the wrong way. [There was no truth to the rumor that Bill Gates had suggested that the planet's rotation be reversed to match his software's description.]

2000-05-26 **Keywords:** elections delay software QA quality assurance

RISKS

**Vol** 20 # 89

In Caracas, Venezuela, the High Court delayed general elections at the end of May because of major problems with election software.





2000-06-05 **Keywords:** software bloat QA quality assurance professionalism RISKS < http://radsoft.net/bloatbusters/sw\_dns.htm >

**Vol** 20 # 91

R. A. Downes examined the source code for an old Microsoft registry cleaner called RegMaid. He trimmed the executable from 153,600 bytes down to 83,968 bytes in ten minutes. "Not to beat the dead horse but - just think about it. Ten minutes, 55% savings of 83,968 - and I had never seen this code before in my life." In another bloatware analysis, his team reduced a piece of commercial software from 3.5MB to 7KB (yes, that's seven \_kilo\_bytes) in a single hour. As Downes wrote, "Avoiding bloat has never been an effort, despite what the defenders of latter-day commercial software like to claim. Things can be done right from the beginning, or even if not, corrected in a negligible envelope of time. . . . It's professional pride on the one side -and `who cares?' on the other."

In a follow-on submission to RISKS, Martin Ward complained about the default handling of inserted images in MS-Word documents: there is no compression unless one takes special measures. As a result, the document ended up at 26 Mb -- when simple compression converted it to a mere 180 Kb. Ward summarized two specific design flaws as follows:

- \* Their image file format doesn't compress images;
- \* MS Word doesn't compress files when it stores them.





2000-07-28 **Keywords:** QA quality assurance design outsourcing consultants failure delay costs RISKS

**Vol** 20 # 98

Peter G. Neumann summarized a software development disaster: "San Mateo County has spent \$35 million thus far on a new Health Services computer system (now two-years old) that was expected to integrate 40 different stovepipe entities that previously were unable to communicate with one another. Over the past few months, the system has been so unreliable that it could not even send out medical bills. The backlog of account receivables is now more than \$40 million. Blame is being distributed among poor initial outside advice, a sudden cut in anticipated money, and damaging turnover in consultants. The costs are about double what had been budgeted." Dr Neumann added, "As an aside that seems relevant to many other situations if not to this one, outsourcing of responsibilities (from requirements to design to implementation to operation and maintenance) is increasingly popular, but doomed if you don't have serious in-house competence to understand what is being outsourced."

2000-08-10 **Keywords:** QA quality assurance

RISKS

**Vol** 21 # 01

Peter G. Neumann wrote, "After problems with its new computer system, Northeastern University unintentionally admitted 25 percent too many freshmen -- 600 extra students -- for this fall. Earlier, the names of hundreds of potential applicants had been lost when the system was first installed, which resulted in an aggressive campaign to enroll the students who had been accepted."





2000-08-11 **Keywords:** quality assurance software bugs

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/cutting/techwr/20000811/tCB00V0452.html>

#### Vol #

A project at eBay to improve the online auction company's computer system is being blamed for at least two system problems in the last few days. Unhappy eBay customers have been expressing their frustration on various online message boards. (Los Angeles Times 11 Aug 2000)

2000-08-29 **Keywords:** quality assurance hardware chip design fabrication

 $News Scan \ (reprinted \ with \ permission), \ Washington \ Post < http://www.washingtonpost.com/wpdyn/articles/A40772-2000 Aug 29.html>$ 

#### Vol #

Intel is recalling its 1.3 gigahertz Pentium III chip, which it has sold only to "a handful" of "power users" running advanced applications, because a certain combination of data, voltage, and temperature conditions may cause the chip to fail. The chip is expected to be back on the market in a couple of months. (Reuters/Washington Post 29 Aug 2000)





2000-09-20 **Keywords:** QA quality assurance boundary condition inequality operator disjunction design testing Web

**RISKS** 

**Vol** 21 # 05

Andrew Koenig reported an interesting boundary-condition problem with some ordering software at an e-commerce site. An Amazon.com e-mail announced a \$50 discount on any order of \$100 or more from the site in question. However, it was impossible to persuade the order software to accept the special discount for a \$100 watch. Solution: a customer-service rep added one penny to the price and succeeded in getting a discounted price of \$50.01. The most likely explanation: someone programmed "> \$100" for the discount instead of "> = \$100." [Moral: follow QA guidelines and test boundary conditions!]

2000-10-19 **Keywords:** QA quality assurance vulnerabilities alerts correction patch

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/zd/zd5.htm >

Vol #

The Swedish security firm Defcom is saying that some large companies have been slow in correcting security vulnerabilities they've been warned about. Defcom's chief technology officer says: "We have found vulnerabilities in major operating systems. More than one company hasn't responded with anything... It is quite irresponsible." Recently, the U.S. government's Computer Emergency Response Team (CERT) decided that in future it will give companies no more than 45 days to fix security problems before it publicizes them. (ZDNet/USA Today 19 Oct 2000)





# **Quality assurance (security products)**

2000-01-09 **Keywords:** Web privacy programming error data leakage

RISKS, AP, SecurityPortal, ZDNet <

http://www.zdnet.com/zdnn/stories/newsbursts/0,7407,2419486,00.html >

Vol 20 # 74

Northwest Airlines warned customers who placed orders on its Frequent Flier Web site that their transactions had been transmitted through the Net in the clear. Seems that Secure Sockets Layer (SSL) was not turned on again after system maintenance in mid-December. An observant customer noticed the unlocked lock symbol in his browser and alerted the company to the problem. No one knows if any credit card numbers or personal data were compromised.

2000-02-21 **Keywords:** fraud separation of duties automatic processing QA quality assurance design liability

**RISKS** 

Vol 20 # 81

Banks in California announced that they would no longer honor requirements for dual-signature accounts. Claiming that automated recognition equipment could not handle dual signatures, the banks refused any liability for allowing unauthorized single-signature withdrawals. The banks thus put many organizations at risk of fraud, especially non-profit groups.





 $2000 \hbox{-} 02 \hbox{-} 23 \qquad \textbf{Keywords:} \qquad \text{Web software QA quality assurance failure password script}$ 

**RISKS** 

**Vol** 20 # 87

When a user entered an invalid request on the Palm Store (palmorder.modusmedia.com), he received an error message that included the system administrator password for the server involved.

2000-03-19 **Keywords:** anti-piracy software QA quality assurance beta failure error bug reboot loop

**RISKS** 

**Vol** 20 # 85

Malcolm Park, writing in the RISKS Forum, reported on a quality assurance failure in the software for reading "free" books downloaded from the Internet. The only format that he was able to receive was the GlassBook, requiring a 7Mb free software download of the appropriate reader. Upon installing this reader, Park's Windows NT4 SP6a operating system went into an endless loop of reboots. By examining his NT partition for a good two hours, Park determined that the fault lay in the InterLok anti-piracy software. As he wrote, "My PC had been crippled by anti-piracy measures applied to a "free" software product I'd installed to read a "free" book. It is entirely feasible that others were locked out of their systems for good by this software."

[Moral: before installing software, be sure you have the necessary recovery tools to reinstate a known-good version of the operating system.]





2000-03-24 **Keywords:** credit-card fraud QA quality assurance CGI programming error vulnerability hole

**RISKS** 

**Vol** 20 # 85

Martin Minow, a regular contributor to the RISKS Forum, reported on vulnerabilities in Perl scripts used to accept credit-card information from consumers. Apparently, in many cases, a simple "update account" will reveal the latest versions of these forms as recently filled in by a customer. The vulnerability results from leaving the CGI script world-readable and in a world-readable directory, just as the vendor supplied it by default. [Moral: always check the default values for adequate security and secure your resources according to your own needs.]





2000-04-14 **Keywords:** QA quality assurance Trojan horse unauthorized code Easter egg vulnerability backdoor

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/ap/docs/4267471.htm>; RISKS

Vol 20 # 88

A three-year-old piece of Microsoft software includes a secret password that could be used to gain illegal access to hundreds of thousands of Web sites, including site management files that could lead to customers' credit card numbers. The code was discovered by two security experts who found within the code the following message: "Netscape engineers are weenies!" Microsoft is urging customers to delete the file, titled "dvwssr.dll," and plans to send out an e-mail bulletin and post a warning on its Web site describing the security hole. (AP/San Jose Mercury News 14 Apr 2000) However, Russ Cooper of Bugtrag wrote in RISKS, "the public has been overly warned against an extremely limited threat... while the real threat from the dvwssr.dll has been largely ignored by the media." Cooper explained that the more important issues were that (1) analysts were able to exploit the dll for buffer overflows; and (2) "While this particular program had minimal use in its lifetime, the fact that a static password (used for obfuscation, not entry) was even present should not be understated. This program has survived numerous Q&A cycles and, if we believe that source code for NT has been available at some 30+ U.S. Universities for years, numerous code reviews."

2000-05-19 **Keywords:** antivirus false positives QA quality assurance

**RISKS** 

**Vol** 20 # 89

The Norton AntiVirus signature file dated 2000-05-18 caused many false positive identifications of the VBS.NewLove.A e-mail enabled worm.





2000-05-25  $\,$  Keywords: antivirus QA quality assurance confidentiality

**RISKS** 

**Vol** 20 # 89

A home-grown anti-virus scanner at a company accidentally converted all e-mail file access attributes to world-readable while it scanned in-boxes for suspect files. The breach of control was discovered only after about 10 days of vulnerability.

2000-05-30 **Keywords:** antivirus quarantine QA quality assurance technical support

RISKS

**Vol** 20 # 90

Richard Thieme, a regular contributor to the RISKS Forum, reported that Symantec's Systemworks 2000 Anti-Virus program reacted to the source code for the network.vbs worm by quarantining an entire Eudora Pro e-mail box where filters automatically stored incoming e-mail from a security list. That entire folder remained permanently inaccessible. When he finally reached a human being in technical support after hours of trying to get a meaningful response on how to recover the quarantined e-mail messages, he was told that no one had ever requested that particular function before. Given that the messages were not, in fact, infected, the anti-virus product actually caused harm instead of preventing it.





2000-07-06 **Keywords:** QA quality assurance

**RISKS** 

**Vol** 20 # 94

CTS, the company that supplies automated barriers for access control to trains in Surrey, England, upgraded the software in June. Instead of improving the response speed, the newly programmed barriers erased the information on valid tickets, causing immense tie-ups for manual restitution to furious customers as well as for manual verification of unerased tickets. [Comment: how could any software firm test so poorly that such a drastic error could slip through quality assurance?]

2000-07-18 **Keywords:** access control QA quality assurance design flaw danger emergency

RISKS

**Vol** 20 # 95

The designers of subway access-control systems have justifiably introduced antipassback timers so that a magnetic ticket cannot be used immediately after someone has entered the restricted area of a station. However, Boyd Roberts reported to RISKS that the London Underground engineers foolishly introduced a timer for egress as well as ingress. Roberts wrote, "This is atrocious design" and pointed out that in an unmanned station, such restrictions on egress could be catastrophic in an emergency.

In a follow-up posting, Clive D. W. Feather explained that the barrier system is controllable by staff, who can analyze the situation and override any blockage. In addition, all Tube stations must be manned all the time, and if staff leave they are required by policy and procedure to disable the barriers.





2000-08-25 **Keywords:** QA quality assurance encryption bug key escrow

RISKS. PoliTech < http://www.politechbot.com/p-00067.html > , Wired < http://www.wired.com/news/print/0,1294,16219,00.html >

**Vol** 21 # 03

The popular PGP encryption and digital-signature software was shown to include a bug in the key escrow functions that allowed unauthorized access to improperly-encrypted ciphertext.

2000-10-16 **Keywords:** access control software canonical passwords hard-coded cleartext crack RISKS

**Vol** 21 # 09

WinU software from Bardon was claimed to lock down computers using Windows; the company's Web site included a list of large customers using the software. Someone posted a list of hard-coded, cleartext canonical backdoor passwords ("emergency passwords") obtained from the executable files, thus at once rendering the product useless and indirectly helping to supply a list of companies ripe for attack.

2000-12-03 **Keywords:** antivirus signature files QA quality assurance operating system crash RISKS

**Vol** 21 # 13

Peter G. Neumann wrote, "Windows 95, 98, and NT all seem to have crashed under McAfee virus definition file version 4.0.4102. It includes a driver that actually imitates the virus. Network Associates recommended starting in Safe Mode and disabling VirusScan's startup scan."





# Availability issues (not denial of service)

2000-01-25 **Keywords:** availability terms service level agreement contract

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000125/t000007795.html >

#### Vol #

A Microsoft Network subscriber is suing the software giant, claiming that Microsoft overloaded its Internet access service by signing up new subscribers without upgrading its system to accommodate the extra traffic. Microsoft recently ran a promotional campaign promising customers who signed up for three years of MSN service a \$400 rebate for purchases at stores such as Office Depot and Best Buy. The lawsuit, which will be filed in federal court in Chicago next week, charges Microsoft with breach of contract and negligence, and will request that the company upgrade its network. (Bloomberg/Los Angeles Times 25 Jan 2000)

2000-01-31 **Keywords:** availability production down-time

Edupage, New York Times

### Vol #

In late January 2000, the National Security Agency's computer systems failed for 72 hours. Not surprisingly, the NSA declined to explain exactly what went wrong, other than to say it was neither a cyberattack nor a Y2K bug.





2000-02-21 **Keywords:** Web site availability offline

**RISKS** 

**Vol** 20 # 81

Shortly after President Clinton announced, "Our administration has been working for years now to reduce vulnerabilities in government computers and to encourage the private sector to do more," the US Senate's Web site went offline for nine hours on the 14th of February.

2000-03-18 **Keywords:** cable back-hoe attack splicing testing cut break availability interruption RISKS

**Vol** 20 # 84

Peter G. Neumann wrote in RISKS: 1,000 phone lines in northeastern San Jose were down for about a week on 10 Mar 2000, when a construction crew accidentally took out four buried cables. `The repair work is mind-numbingly tedious, with each wire having to be spliced by hand and then tested.' [Source: \*San Francisco Chronicle\*, 14 Mar 2000, A13,18, PGN-ed]





2000-03-22 **Keywords:** backhoe attack optic fiber availability outage

**RISKS** 

**Vol** 20 # 85 & 86

Tim Dixon wrote as follows in RISKS:

"When will people learn? Computerworld reports that Northwest Airlines had to cancel about 130 flights during a 3.5-hour outage at their Twin Cities hub. It seems a contractor accidentally bored into the cable cluster containing both main and redundant fibre lines.

[http://www.computerworld.com/home/print.nsf/CWFlash/000322CBDE]

When will people learn they need to know where their redundancy lies? Cables run through the same conduit are only partially redundant, as events like this will happily take out all the cables in a conduit, making the conduit itself a single point of failure."

2000-04-05 **Keywords:** bandwidth technology protocols network broadband consortium NewsScan (reprinted with permission)

### Vol #

A group of more than 30 companies, including Nortel, AT&T, NBC Internet, Bertelsmann, Qwest, Sun Microsystems and British Telecom, are working together to design communications architectures for broadband networks. The Broadband Content Delivery Forum hopes to speed up access to high-bandwidth content by using so-called co-location centers near ISPs, which would alleviate bottlenecks in long distance networking traffic. It will also focus on "content mediation" technologies that enable providers to recognize their subscribers and offer them highly personalized content and services. Noticeably absent from the group are Cisco and Lucent, which have been invited to join, but may instead prefer to set their own industry standards. (Financial Times 5 Apr 2000)





2000-04-13 **Keywords:** availability backup failure power airport travel disruption air traffic control

**RISKS** 

Vol 20 # 87

A power failure at 19:50 on 2000-04-10 affected Washington National Airport.. The backup generator failed at 20:41 and power was not restored until  $\sim$  04:00 the next morning. The outage severely affected travelers and nearby hotels were swamped with stranded would-be passengers. Peter G. Neumann commented in RISKS, "Yes, they needed backup to the backup."

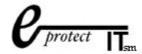
2000-05-14 **Keywords:** remote control automobile shutoff risk counterfeit hacking traffic chaos infrastructure protection

**RISKS** 

**Vol** 20 # 89

RISKS contributors Serguei Patchkovskii and John Pettitt both remarked on a stupid idea for stopping automobiles: a remote-control device using a receiver in each vehicle that could shut off the electrical system of the car at the push of a button. News reports apparently failed to note (1) the risks to other vehicles from cutting off power to a speeding automobile in a heavily-traveled lane; (2) the risks of counterfeit control devices. Pettitt wrote, "There is so much wrong with this idea it's hard to know where to start; even if the system was designed well enough that only "real" guns would work (very unlikely IMHO) a stolen "gun" could create total gridlock in a city."





2000-06-19 **Keywords:** availability bandwidth music trafficking network congestion satellite alternative

Edupage, NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB953765627187819503.htm>

### Vol #

In January, Oregon State University administrators banned the Napster program from its networks, saying that the enormous volume of stolen songs was exceeding its bandwidth budget. Calculations showed a doubling time of only three months if the growth in song traffic were to continue unabated.

[In March,] Napster . . . adapted its software to use more "intelligent" search techniques and thus streamline the bandwidth needed to download requested files. The software change, which is the result of an unusual collaboration between the fledgling company and Indiana University, one of the first colleges to block the program, takes advantage of the fact that many colleges are now connected to the high-speed, next-generation Internet2. Now, when a Napster user asks for a file, the software first looks for the file on the user's campus network, then on the high-speed network. Those downloads take much less time than ones from the public network, thus reducing the load on the university networks. As a result, Indiana University . . . [said it was] ready to allow Napster back on campus . . . although network operators . . . [would] continue to monitor its use. (Wall Street Journal 23 Mar 2000)

Ever since MP3 music files took college campuses by storm, the problem of traffic congestion on campus networks has been growing. A typical case is Bucknell University, where 40% of the school's total Internet traffic is attributable to MP3 download services such as Napster. In an effort to resolve the gridlock, Bucknell officials called on alum Jeff Boulter, now a senior director of product development at Launch Media, to come up with a solution. The result is Launch College Direct, a service that uses iBeam Broadcasting's proprietary system to stream Internet content via satellite and put it on a local network that bypasses the school's Internet connection. The new service, which is free, will be deployed first at Bucknell and Georgia Tech. Launch plans to use it to deliver its own collection of music and music videos. (Los Angeles Times 19 Jun 2000)





2000-08-25 **Keywords:** availability DNS Domain Name Service servers access RISKS

**Vol** 21 # 03

When four of the 13 root servers at Network Solutions Inc failed, worldwide access, including HTTP, FTP, and SMTP, to all sites in the ".com" domain was interrupted for an hour, .

2000-09-07 **Keywords:** electric power availability infrastructure protection NewsScan (reprinted with permission)

Vol #

Technology experts Peter Huber and Mark Mills charge that politicians have been ignoring a growing crisis caused by an energy-guzzling computer industry: "A personal computer and its peripherals typically boost power consumption in your home by about 5% per year — more if you run with the Wired crowd. But most of digital infrastructure's burgeoning demand for power occurs out of sight. Almost all the power it takes to deliver a conventional TV picture is used in the den where you watch it. The Web's invisible infrastructure, by contrast, consumes at least twice as much power as the hardware on your desktop. A Palm Pilot sips tiny amounts of power — but connect it to the Web and it can add as much new electric load as a refrigerator, in the servers, routers, and digital transmission systems used to feed it... A year ago we estimated that some 13% of U.S. power output was being used to manufacture and run computers and the sprawling infrastructure. It's more than that today. The country is 'siliconizing' everything — and behind every digital bit stands a bucket of electrons, behind every chip a power supply." Huber and Mills are coauthors of the Digital Power Report, a newsletter. (Wall Street Journal 7 Sep 2000)





2000-10-12 **Keywords:** availability electrical power process control bug error failure RISKS

**Vol** 21 # 09

At Eastbourne General Hospital, a computer-controlled backup electrical generator was prevented from cutting in to the circuits when mains power failed because the software appeared to "think" that the backup was already online. Later, when mains power actually was restored, the software prevented it from reaching the operating rooms because it "thought" that the backup generators were still running. As a result of the power interruption, medical staff had to complete a Caesarian section by flashlight ("torchlight" for British readers).

2000-12-03 **Keywords:** availability crash mainframe banking financial transactions stoppage outage

**RISKS** 

**Vol** 21 # 15

Peter G. Neumann summarized a report by Sam Zuckerman in the \_San Francisco Chronicle\_ of the 2nd of December: "On 1 Dec 2000, the nationwide Wells Fargo computer network crashed for a few hours, three days after WF had finished merging their computer networks with those of Norwest (which bought WF in 1998). One of four Hitachi Tritium 400 mainframes in the Minneapolis data center shut itself down, apparently after detecting some sort of anomaly. The result stopped all banking operations that depend on real-time interaction."



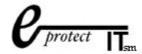


### 24.3 ActiveX

2000-05-24 **Keywords:** mobile code ActiveX vulnerability certificate CERT-CC Advisory < http://www.cert.org/advisories/CA-2000-07.html > **Vol** 2000 # 07

CERT-CC reported, "The Microsoft Office 2000 UA ActiveX control is incorrectly marked as "safe for scripting". This vulnerability may allow an intruder to disable macro warnings in Office products and, subsequently, execute arbitrary code. This vulnerability may be exploited by viewing an HTML document via a web page, newsgroup posting, or e-mail message." The vulnerability applied to all systems with Internet Explorer and any Microsoft Office 2000 products. One interesting aspect of the case is that the vulnerability was first reported to CERT-CC by L0pht Research Labs and @Stake, supporting the view that the pseudonym-using staff of those organizations are genuinely committed to professionalism. More important, however, is that the vulnerability exposes the fundamental weakness of the entire security model for ActiveX: knowing where a control originates in no way guarantees the safety of that code.





2000-12-22 **Keywords:** activeX security workshop paper publication report RISKS, CERT-CC < http://www.cert.org/reports/activeX\_report.pdf >

**Vol** 21 # 17

Richard M. Smith wrote, "This past summer, CERT sponsored a two-day workshop on security issues with ActiveX controls. The final report was just released today and is available as a PDF file at the CERT Web site: <

http://www.cert.org/reports/activeX\_report.pdf > . There is a lot of good information in the report about how individuals and organizations can reduce security risks in Internet Explorer when using ActiveX controls. In addition, there is a section aimed at software developers on how to create safer controls.

A good bit of the technical information in the report has not been made public before."





### **24.4** HTML

2000-02-03 **Keywords:** alert CERT-CC FBI DOD Web cross-site scripting vulnerability NewsScan (reprinted with permission)< http://www.msnbc.com/news/365542.asp>

Vol #

Carnegie Mellon U.'s CERT Coordination Center, together with the FBI and the Defense Department, has issued a warning citing a security flaw in most complex Web sites that could allow hackers to launch malicious programs on a person's computer or capture information disclosed by a Web site user, such as credit card numbers. The flaw involves "cross-site scripting," which enables dangerous computer code to be embedded in innocuous-looking links to popular Web sites. The vulnerability is not limited to any particular kind of software, and occurs when complex Web sites fail to verify that hidden software code sent from a consumer's browser is safe. "Any information that I type into a form, what pages I visit on that site, anything that happens in that session can be sent to a third party, and it can be done transparently," says top Microsoft security manager Scott Culp. CERT says only a massive effort by Web site designers can remedy the problem, but in the interim, users should avoid clicking on Web links from untrusted sources, such as unsolicited e-mail messages or discussion forum messages. (AP/MSNBC 2 Feb 2000)

Peter Neumann, moderator of the RISKS Forum, added that the alert would be available at < http://www.cert.org/advisories/CA-2000-02.html > and that readers might also want to read the FAQ at <

 $http://www.cert.org/tech\_tips/malicious\_code\_FAQ.html > .$ 





2000-02-03 **Keywords:** shopping cart vulnerability data diddling TheRegister.com < http://www.theregister.co.uk/000203-000006.html >

Vol #

According to Internet Security Systems (ISS), 11 shopping-card software packages in use on the Net allow hackers to modify prices of goods when they are added to the order. One vulnerability involves using hidden fields in HTML forms to hold information about the products sold; since it is possible to see and modify HTML source locally, criminals can alter the prices before ordering. Another hole involves similar fields for discount information. A third occurs when programmers put the price in the URL, so that altering that parameter alters the price for the shopping cart.

2000-03-29 **Keywords:** privacy covert channel monitoring identifier continuity Web browser behavior HTTP programming spyware

**RISKS** 

**Vol** 20 # 86

Martin Pool explained a newly-discovered exploit for surreptitiously monitoring the behavior of Web-site visitors. Much like cookies, the headers of cached objects are returned to a Web server when the browser checks to see if there have been any changes to specific objects (if there are, the browser downloads a new copy; if not, the browser uses the cached copy of the object). If an unscrupulous Web-site programmer stores unique information in the Last-Modified field of stored objects, the behavior of tagged users (or at least, of users of a specific browser on a particular computer) can be monitored. Because the Last-Modified field is returned only if the browser client requests exactly the same URL (and all associated parameters), the snooping HTML programmer has to provide an object that will not change and that is common to all pages on the site; an example would be a (near-invisible) single pixel. Using the full extent of the Last-Modified field, snoopers would be able to generate approximately 1B unique identifiers per object — and each new object would offer the opportunity for another billion identifiers.





2000-07-31 **Keywords:** QA quality assurance Web site source testing tool editor concealment distortion trickery compensation bad design standards interoperability

**RISKS** 

**Vol** 20 #

Lloyd Wood reported on a dangerous feature of Internet Explorer 5.5: it alters the appearance of HTML source code by suppressing the visibility of embedded backslashes. He discovered this extraordinary deception when he tried to figure out why the non-standard (invalid) HTML code one of his colleagues generated using MS-Word was failing with other browsers but working in IE. As he wrote in RISKS, "If you view source, you expect to see the actual source, and not a prefiltered version. This filtering is clearly a risk in that it allows behaviour that would previously have been clearly exposed as bugs in the composing products to stay, unnoticed and uncorrected, because it means you can't trust the tool you're using, and because it screws up interoperability testing. (Which, because IE comes from Microsoft, is hardly a surprise.)"

2000-09-20 **Keywords:** denial of service filtering censorship HTML-enabled e-mail attack vulnerability

RISKS

**Vol** 21 # 05

Dan Birchall noted in RISKS that HTML-enabled e-mail could be used to cause trouble for anyone behind a proxy server equipped with anti-porn (or other) censorware. By embedding invisible pixels addressing banned sites in such e-mail, an attacker could generate an arbitrary number of entries in the censorware log files, thus initiating investigations of specific victims. The poor souls under investigation would have no idea that the e-mail they had received was surreptitiously harming their reputations.





2000-11-22 **Keywords:** e-mail monitoring spyware covert channel privacy hostile code HTML Web bugs

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/2000/11/22/technology/22NET.html >

### Vol #

Privacy advocates are concerned about the fact that the new e-mail software system called HTML mail makes it possible for people sending you messages to monitor when and what time of day you open them, how often you reopen them, and whether you forward them to other people. The marketing companies that use HTML mail say it helps them develop more personalized promotions; individuals who use it claim they have a right to monitor their own correspondence. Richard M. Smith, the chief technology officer for the Privacy Foundations, argues: "You can buy 50,000 addresses of people who subscribe to The New Yorker. But you don't know what articles they're reading in it, or what books they've bought or what medical problems they've been researching lately. That's very much a possibility within this technology." (New York Times 22 Nov 2000)





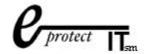
## **24.5** E-mail

2000-04-27 **Keywords:** e-mail execution arbitrary code e-mail URL link vulnerability hole RISKS; Peacefire < http://www.peacefire.org/security/stealthattach/ >

Vol 20 # 88

Peacefire reported a new class of exploits using e-mail to force execution of arbitrary code by the Eudora e-mail client when a user clicks on an embedded URL in an HTML-enabled e-mail message. Bennett Haselton, writing in RISKS, said, "Security holes that allow you to run code on a remote user's machine just by sending them e-mail, are extremely dangerous -- a hacker could use this to steal or erase any classified data on a remote user's hard drive, even if that user were behind a corporate firewall and had anti-virus software running. A virus writer could use the exploit to write a virus that could spread to almost all Eudora users -- numbering in the millions -- and potentially do hundreds of millions of dollars' worth of damage. (Unlike most such tricks, this exploit does not require the user to do anything "naive", like run an .exe that is sent to them as an attachment.) USA Today reported last year on the "BubbleBoy" virus, which similarly used a security hole in Microsoft Outlook to cause code to run on a user's machine, simply by reading an e-mail message"





2000-05-05 **Keywords:** QA quality assurance design flaw programming language functionality RISKS, BBC < http://news.bbc.co.uk/low/english/sci/tech/newsid\_737000/737396.stm > **Vol** 20 # 88

Russ Cage noted a rare burst of insight in the non-technical press about the fundamental reason there are e-mail enabled worms floating around cyberspace: the decision by Microsoft to include programming functionality as part of its office products. Writing in RISKS, he quoted from a BBC news article as follows: "Peter Sommer... told BBC News Online that Microsoft created these by building in to their software the tools needed to customize applications. Microsoft customers are going to have to ask the company to review very carefully the level of functionality that they are putting into their systems. [...] One has got to ask why products are put out which contain these programming languages, which may be of use to perhaps only 3 to 4% of the customers but for everyone else presents a considerable threat. [...] These features are also very difficult to turn off. The lesson from Love Bug is that people must be able to kill off this programming functionality within applications programs."

2000-06-14 **Keywords:** anti-virus security sandbox restriction script limitations e-mail worms patch fix improvement

RISKS, Reliable Software Technologies < http://www.rstcorp.com/news/jbf.html >

**Vol** 20 # 92

Gary McGraw announced, "Reliable Software Technologies has just released a new program (JustBeFriends) designed to prevent e-mail macro viruses from spreading. It can be used along with or instead of the Microsoft supplied e-mail protection patch. JustBeFriends works will all versions of Outlook and Outlook Express, and is substantially simpler than the Microsoft patch." The program prevents all automated, script-based access to Outlook programs, thus blocking the mechanism used by e-mail enabled worms.





# 24.6 Web-site infrastructure, general Web security issues

2000-05-15 **Keywords:** Web programming QA quality assurance vulnerability fix RISKS, Zope < (http://www.zope.org/Members/jim/ZopeSecurity/ClientSideTrojan > **Vol** 20 # 89

Chris Adams summarized a widespread vulnerability in Web-site administration tools: "Basically, an attacker could create a page that redirected to site's admin interface or a form that submitted to it (possibly using JavaScript for automatic submission); in any case, the effect was that any use who was logged in as a site administrator could have an attacker execute arbitrary commands in their security context merely by following a link. If this was carefully set up using JavaScript and frames, it's more than possible that the admin would never notice what had happened. This attack would be particularly effective against online news sites and anyone else for whom it is common to receive many URLs every day as submissions." Adams pointed out that an easy fix was to make it more difficult to guess the form parameters for generating the URLs: "given that you need to have a random identifier that is not leaked to third parties for meaningful session management, an obvious step is to put in a parameter in the form that must match the user's session ID (e.g. Confirm=346593045 instead of Confirm=true)."





2000-05-26 **Keywords:** cache certificate user interface error QA quality assurance design flaw vulnerability exploit

RISKS, CERT-CC < http://www.cert.org/advisories/CA-2000-08.html >

**Vol** 20 # 89

Kevin Fu reported in RISKS that Netscape Navigator has a flaw in the user interface for dealing with invalid certificates: "Within one Netscape session, if a user clicks on "continue" in response to a "hostname does not match name in certificate," then that certificate is incorrectly validated for future use in the Netscape session, REGARDLESS of the hostname or IP address of other servers that use the certificate. It seems that the "Certificate Name Check" warning will cache a certificate as valid for any hostname or IP address in the future. In this way, if an adversary tricks a user into accepting an invalid certificate at a seemingly benign site, then the user can then be tricked if he/she ever visits a malicious site using the same certificate. A `continue' click on a seemingly benign SSL web server might end up taking away server authentication from visiting https://www.a-site-that-you-give-private-info.com/ that has poisoned DNS." Fu concludes that this case raises serious questions:

- (1) A user interface should be explicit; "Continue" is an insufficient indicator of function.
- (2) Implementing security is hard, and the failure of Netscape should raise warning flags about implementation by other companies who invent their own security solutions.





2000-06-01 **Keywords:** malicious code executable compression stupidity risk management sneakernet air gap copyright UCITA license dissemination control

**RISKS** 

**Vol** 20 # 90

Avi Rubin complained in RISKS about how Microsoft distributed a white paper -- by offering a self-extracting executable file. "Of all companies, Microsoft should be the last one to encourage users to get into the habit of downloading .exe programs and running them. . . . The problem is that it is very difficult to know that a program is harmless, just because it does something that you expect it to do. I could not believe that this is how Microsoft distributes its white papers. It is beyond comprehension."

In the next issue of the RISKS Forum Digest, Paul Wallich suggested that putting a document into an executable file might be a way of restricting distribution: "Bundling the file into an executable, however, arguably meets the requirements of the Digital Millennium Copyright Act for a technological copy-protection mechanism, which makes unauthorized redistribution of the text a serious crime (where `serious' means `you could go to jail for more than a year'). . . . If you view control, rather than dissemination, as the goal of putting documents on a web site, it's easy to comprehend."

2000-06-29 **Keywords:** confidentiality Web security failure

**RISKS** 

Vol 20 # 94

Keith Rhodes reported in RISKS, "In Australia, someone claimed to have accessed a Treasury Department Web site www.gstassist.gov.au that had essentially no security. By indexing from 1 to 17,000, he was able to obtain the bank records of that many registered GST Startup certificate suppliers. (There were apparently 27,000 records in all, but access stopped when the site was disabled.) He then sent e-mail to each these companies (which can honour a \$200 GST-related rebate on computers, software, services and other items required for small and medium companies to prepare for Australia's new taxation system) with its own relevant details."





2000-07-18 **Keywords:** QA quality assurance Web design encryption false information cleartext transmission

**RISKS** 

**Vol** 20 #

The Royal Mail Web site claimed that it was using encrypted traffic to capture credit-card information when in fact it was not. An alert RISKS contributor, Gary Barnes noticed that his browser was in HTTP mode rather than HTTPS mode. Two weeks after he reported the problem, the incorrect protocol and the incorrect assurance of security were still in place. He wrote, "The RISK here is that customers will believe a web site that says `all orders sent from your computer to our servers [...] will be secured through the use of encryption technology', especially when the organisation responsible is as `trustworthy' as Royal Mail, and then trustingly send their unencrypted card details over the Internet. There's also the RISK that once alerted to such mistakes companies won't or can't act to fix the problem in a timely fashion, or at least remove their incorrect boasts of being `secure'."

2000-08-03 **Keywords:** confidentiality passwords e-mail access design Web security flaw vulnerability management process operations

RISKS

**Vol** 21 # 03

During the month of July, an internal search page allowing access to user IDs and passwords was made world-readable on Switzerland's second-largest ISP. Over 700 accounts were compromised on the Sunrise ISP due to at least 20 different searches. Such a lapse is a violation of the European Directive on Data Privacy. Peter Kaiser, writing in RISKS, pointed out that storing unencrypted passwords is a terrible idea, let alone when the only protection was security by obscurity. He also pointed out to the ISP that their practice of soliciting user passwords in unsecured HTTP (instead of HTTPS) was a bad idea, but his warnings were ignored.





2000-08-16 **Keywords:** Web site URL ID strings data diddling modification access public relations privacy

**RISKS** 

**Vol** 21 #

The dangerous practice of encoding identifiers in URLs was exposed once again by Paul van Keep in RISKS, who reported that the < annapa.com > Web site allows anyone to alter the identifier in the URL for an account to access other accounts. Unfortunately, the company belittled the exploit, claiming that it was somehow restricted to "IT-specialists" only and therefore not a significant vulnerability.

2000-08-17 **Keywords:** Web site security log files accessibility access controls attributes RISKS

**Vol** 21 # 02

The Canadian \_Globe and Mail \_ (sometimes referred to as the \_Groan andWail\_) Web site has world-readable log files that record, among other things, the exact IP address and search string of every request.

2000-08-25 **Keywords:** user identification policy problem vulnerability error flaw design stupidity confidentiality

RISKS

Vol 21 #

Hotmail makes buddy lists available to anyone who registers an e-mail account using the name of an expired account. However, as Jay Ashworth noted in RISKS, more important is that allowing reuse of an identifier opens up enormous potential for impersonation and fraud.





2000-08-27 **Keywords:** Web design flaw inconsistency

**RISKS** 

**Vol** 21 # 04

Daniel P. B. Smith noted in RISKS that the eBay online auction Web site shows a time counter on each auction's Web page. Unfortunately, although the counter is updated in real time, the rest of the status information -- including how many bids there are -- does not get updated as frequently. He goes on to describe an embarrassing situation where he accepted an early, lower bid because he never received updates from eBay about a later, higher bid.

2000-10-03 **Keywords:** Web design glitch bug unknown access typo search confidentiality world readable medical information

**RISKS** 

**Vol** 21 # 09

Mistyping a search keyword on the Florida Department of Health's Web site caused the mystified user to access sensitive files including names, addresses and medical information. The state CIO apologized for the glitch and said the Health Department would continue investigating the glitch to find the cause and stop recurrence of such errors.

2000-10-24 **Keywords:** Web design flaw URL confidentiality

**RISKS** 

Vol 21 # 09

The New Jersey EZPASS Web site was shut down after it became clear that anyone could access the billing information for other users by altering a URL to transform it into someone else's URL. [MORAL: don't design Web sites so that identification information is encoded in URLs.]





# Remote control, jamming (not interception), RFI, HERF, EMP/T

2000-01-06 **Keywords:** RFI radio frequency interference jamming hijacking BBC < http://news.bbc.co.uk/hi/english/sci/tech/newsid\_592000/592972.stm >

Vol #

Some car radios in Britain are equipped with circuits that automatically switch to specific frequencies so that drivers can hear emergency road reports. Unfortunately, pirate radio-station operators have discovered how to misuse the Radio Data System (RDS) to their own advantage. They constantly transmit the data signal, forcing the radios to stay tuned to the pirate frequencies until the cars leave the local transmission area or the driver disables the RDS feature. Authorities were hunting the pirates.





# 25.1 Remote control

2000-05-31 **Keywords:** remote control radio frequency interference RFI hacking vulnerability risk design

**RISKS** 

**Vol** 20 # 90

The General Motors OnStar system will allow not only geographical positioning data, local information, and outbound signaling in case of accidents: it will also allow inbound remote control of features such as door locks, headlights, the horn and so on -- all presumably useful in emergencies. However, Armando Fox commented in RISKS,

> If I were a cell phone data services hacker, I'd know what my next project would be. I asked the OnStar speaker what security mechanisms were in place to prevent your car being hacked. He assured me that the mechanisms in place were "very secure". I asked whether he could describe them, but he could not because they were also "very proprietary". \*Sigh\*<





2000-08-17 **Keywords:** information warfare battlespace remote-control armament police law enforcement equipment robot Internet vulnerability risk

**RISKS** 

**Vol** 21 # 02

Anatole Shaw reported in RISKS on a dreadful new development in mobile attack weapons: "The Thailand Research Fund has unveiled a new robot, resembling a giant ladybug with a couple of extra limbs. The unit is equipped with visible-spectrum and thermal vision, and a gun. According to Prof. Pitikhet Suraksa, its shooting habits can be automated, or controlled `from anywhere through the Internet' with a password. The risks of both modes are obvious, but the latter is new to this arena. Police robots of this ilk have been around for a long time, but are generally radio-controlled. The apparent goal here is to make remote firepower available on-the-spot from around the Internet, which means insecure clients everywhere. How long will it take for one of these passwords to be leaked via a keyboard capture, or a browser bug? Slowly, we're bringing the risks of online banking to projectile weaponry."

2000-08-25 **Keywords:** remote control cellular telephones wireless mobile active content RISKS

Vol 21 #

Several hundred users of new Japanese programmable wireless phones were harassed when someone remotely ordered their devices to dial the emergency services. Kevin Connolly commented in RISKS, "The risk is that people designing new mobile phone functions do not learn from the mistakes in the MS Word macro `virus enabling' feature."





2000-10-20 **Keywords:** remote control laboratory equipment Internet hacking

RISKS

**Vol** 21 # 10

A gateway sold by National Instruments allows instruments equipped with the standard IEEE-488 bus to be connected to the Internet -- completely without any security provisions -- and thus controlled remotely by total strangers. The usual dangers to the electronic equipment are exacerbated, wrote Stephen D. Holland in RISKS, because laboratory equipment is often used to control mechanical devices.

2000-12-22 **Keywords:** remote control reconfiguration firmware upgrade automatic modification control integrity error QA quality assurance design

**RISKS** 

**Vol** 21 # 17

In the early 1990s, certain tape drives were criticized for allowing uncontrollable automatic firmware upgrades if a "firmware-configuration tape" was recognized. The problems occurred when the tape drive "recognized" a tape as such even if it wasn't. A decade later, the same type of feature -- and problem -- has been noted in Dolby digital sound processors for the audio tracks of 35mm film: any time anything looking like a firmware-reconfiguration data stream is encountered, the device attempts to reconfigure itself, regardless of validity of the data stream or the wishes of the operator. A German contributor to a discussion group about movie projectors noted (translation by Marc Roessler), "The trailer of "Billy Elliott" has got some nasty bug: If the trailer is being cut right behind start mark three, the CP500 will do a software reset with data upload as the trailer runs through the machine. Either Dolby Digital crashes completely or the Cat 673 is set to factory default, which means setting the digital soundhead delay to 500 perforations, i.e. the digital sound lags 5.5 seconds behind the picture. . . . "





# 25.3 RFI, HERF, EMP/T

2000-05-29 **Keywords:** radio frequency interference RFI avionics cellular phones mobile RISKS; New Scientist < http://www.newscientist.com/nsplus/insight/phones/dangersignals.html > **Vol** 20 # 89

According to a study in Britain's New Scientist magazine, cellular (mobile) phones do in fact exceed radio-frequency interference tolerances for avionics in older airplanes.

2000-06-06 **Keywords:** RFI radio frequency interference control systems electrical

RISKS, Canadian Broadcasting Corporation <

http://cbc.ca/consumers/market/recalls/reclfull/2000/06jun2000b.html >

**Vol** 20 # 91

According to an article on the CBC Web site, Ford Explorers are subject to radio-frequency interference with their central computer, resulting in non-responsive on/off switches. Alex Wiebe wrote in RISKS, "the result is anything ON will stay ON, anything OFF will stay OFF." Wiebe noted that the headline for this article referred to air-bags whereas the body did not; if air bags were affected by electronic noise, the danger to drivers and passengers could be severe.





2000-09-06 **Keywords:** RFI radio frequency interference avionics crash theory

RISKS, NY Review of Books <

http://www.nybooks.com/nyrev/WWWfeatdisplay.cgi?20000921092F >

**Vol** 21 # 04

A report in the New York Review of Books by Elaine Scarry entitled "Swissair 111, TWA 800, and Electromagnetic Interference" suggested that two flights that took off from JFK airport at the same time on Wednesday nights and then crashed may have been affected by strong radio-frequency interference from military installations nearby. However, Professors Peter Ladkin and Willi Schepper of the University of Bielefeld, Germany, published a strong refutation of Scarry's speculations in a paper published on their Web site at < http://www.rvs.uni-

bielefeld.de/publications/Papers/Scarry-refutation.pdf > . These scientists pointed out that the radio-frequency flux would have to be at least 6.8M times greater than anything available in order to trigger explosions inside the plane. Instead, their analysis leads them to focus on the possibility of defective wiring in both planes.





2000-12-26 **Keywords:** RFI radio frequency interference avionics navigation RISKS, The Times of London < http://www.thetimes.co.uk/article/0,,2-58265,00.html > **Vol** 21 # 17

David Kennedy summarized a case of radio-frequency interference for RISKS (quoting his summary verbatim):

ROYAL AIR FORCE pilots will stop using a bad-weather navigation system from January 1 because new commercial radio frequencies have made it unreliable, the Ministry of Defence said yesterday. Pilots of military planes and helicopters fitted with the Instrument Landing System (ILS) will not be allowed to use it to land in poor weather in the new year. Instead they will have to ask air traffic controllers to talk down their flights.

- \* Commercial FM growth cited as cause.
- \* Commercial ILS on different frequencies has not been affected.
- \* Affected aircraft are Nimrod reconnaissance and search and rescue helicopters. RAF transport a/c have already been upgraded and tactical aircraft do not use ILS.

"There is no operational impact whatsoever," a ministry of Defense spokeswoman said. "It is a worldwide problem which affects all countries." "New landing assistance systems use more reliable technology, such as global positioning satellites, which are not affected by radio frequencies. ILS can also be disrupted by signals from mobile telephones."





# 25.4 Health effects of electronic equipment (phones, screens, etc.)

2000-12-08 **Keywords:** RFI radio frequency interference emissions irradiation health hazards danger cellular phones mobile

NewsScan (reprinted with permission), San Jose Mercury News < http://www0.mercurycenter.com/svtech/news/breaking/reuters/docs/723127l.htm >

### Vol #

The British government will invest \$10 million in a research program designed to investigate potential health hazards of cell phones and to mount a public information campaign advising cell phone owners that they should keep their calls short to minimize their exposure to radio waves, and that they should discourage cell phone use by children. Presenting its action as essentially a precautionary step, the government acknowledged that there is no irrefutable medical evidence that cell phones pose health risks.

2000-12-19 **Keywords:** RFI radio frequency interference emissions irradiation health hazards danger cellular phones mobile

NewsScan (reprinted with permission)

#### Vol #

A study of 891 people who used cell phones for up to three years has found no evidence that cell phone use causes brain cancer. The study, which was funded by the industry group Wireless Technology Research and the National Cancer Institute, has been criticized by some scientists for being premature and inconclusive. Professor Henry Lai of the University of Washington says: "Since most solid tumors take 10 to 15 years to develop, it is probably too soon to see an effect." (AP/USA Today 19 Dec 2000)





# Operating systems, network operating systems, TCP/IP problems (alerts)

2000-03-21 **Keywords:** threats operating systems utilities vulnerabilities reports alerts CERT Summary CS-2000-01 < http://www.cert.org/summaries/CS-2000-01.html >

**Vol** 00 # 01

The first edition of the CERT-CC Summary for the year 2000 included warnings of Distributed Denial-of-Service Developments, BIND Vulnerabilities, Multiple Vulnerabilities in Vixie Cron, Root Compromises, and Malicious HTML Tags Embedded in Client Web Requests.

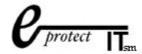
2000-04-09 **Keywords:** software open-source

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/reuters/docs/408434l.htm>

### Vol #

Intel plans to use the Web to give away advanced security software based on industry-standard security functions known as the Common Data Security Architecture. A report in the Wall Street Journal says Intel will begin making the software available by mid-May. (Reuters/San Jose Mercury News 9 Apr 2000)





# 26.1 Windows 9x/Me

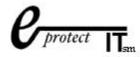
2000-07-19 **Keywords:** Trojan horse buffer overflow e-mail

RISKS, Securityfocus < http://www.securityfocus.com/news/62 >

**Vol** 20 # 97

MS-Outlook and Outlook Express were shown to be susceptible to a buffer overflow through the date field of incoming e-mail. The bug was fixed using the IE SP1 or IE v5.5 on Windows 9x and NT. A service pack was made available for Windows 2000. The buffer overflow would allow execution of arbitrary code upon receipt of e-mail, not through execution of mobile code.





### 26.2 Windows NT/2K

2000-02-20 **Keywords:** QA quality assurance operating system bugs

**RISKS** 

**Vol** 20 # 80

Jim Allchin, Group Vice President, Platforms Group, Microsoft Corporation, wrote an open letter to MS customers about claims that Windows 2000 had over 63,000 defects. He listed a number of threads of evidence showing that Windows 2000 was the most highly tested and stable products the company had released.

2000-02-21 **Keywords:** QA quality assurance availability operating system

RISKS

**Vol** 20 # 81

According to users of a new Windows 2000 system in the Tula County Court Clerk's Office, the new operating system was causing serious downtime: "The new system has been down completely for at least a day twice in the last two weeks and regularly has system errors that hinder access to records for hours at a time."





2000-09-08 **Keywords:** access control vulnerability operating system lock screen saver communications port vulnerability

**RISKS** 

**Vol** 21 # 04

Avi Rubin noted in RISKS that despite the "lock" function in Windows 2000 and Windows NT, communications through ports still works. He illustrated the risks by sketching scenarios in which the synchronization function of the Palm Pilot could be used to obtain or damage information on a supposedly locked system. [Readers should note that under Windows 9x, screen savers, even secure ones, do not generally prevent access via the communications ports if appropriate software is running. LapLink, for example, functions perfectly well even if a target computer is in screen-saver mode.]





# 26.3 UNIX flavors

2000-01-17 **Keywords:** operating system security

Federal Computer Week < http://www.fcw.com/fcw/articles/web-nsalinux-01-17-00.as >

Vol #

In January, the NSA authorized Secure Computing Corporation to develop a secure version of Linux. Contract terms stipulated robust, highly secure operations.





# **26.4** TCP/IP & HTTP

2000-09-25 **Keywords:** availability single point of failure dynamic addressing

RISKS

**Vol** 21 # 07

William P. N. Smith reported in RISKS on an interesting failure of his cable-modem service on the 24th September due to failure of the DHCP (Dynamic Host Configuration Protocol) servers that temporarily assign ("lease") IP addresses to users on TCP/IP networks: "Turns out the DHCP server for the entire northeast went down, and as people's leases on their IP addresses expired, they were dropped off the network. I asked about the secondary or backup DHCP servers, but apparently there was so much demand due to expired leases that the backup server couldn't respond quickly enough, and was getting overloaded with requests."

[A personal note from your editor: I have a secondary ISP with which I contract for only 5 hours a month at a very low cost. Although I use it rarely, it has prevented me from snarling in frustration on the odd occasion when my primary ISP has rejected connections.]

Smith drew two particularly interesting conclusions from this case:

- \* "Even single users ought to have a backup Internet connection" such as a dialup ISP;
- \* "Your backups might have to be more powerful than your primary servers. . . . "





2000-12-16 **Keywords:** Web site redirection spoof HTTP syntax misleading trickery hoax joke RISKS

**Vol** 21 # 16

A hoax taking advantage of a little-used and practically unknown feature of HTTP syntax for URLs convinced many victims that the CNN.com site had been hacked. Rob Warnock explained what happened in a report for the RISKS Forum: "An MIT student named Eric Varady took a parody news article from The Onion < URL:http://www.theonion.com/onion3637/bush\_horrified.html>, edited the layout to resemble CNN's format, and copied it to his own site < URL:http://salticuspeckhamae.mit.edu/evarady/www/top story.htm> ." He then circulated a false story about a hack of the CNN site and pointed people to < URL:http://www.cnn.com&story=breaking\_news@18.69.0.44/evarady/www/top\_st ory.htm>. It turns out that although this URL follows the correct syntax, anyone assuming that the Web page resides on "www.cnn.com" is being misled. The section between the "//" delimiter and the "@" sign is actually interpreted as a \_user\_ field and then discarded. The actual URL is therefore the part following the "@" sign and is therefore equivalent to < http://18.69.0.44/evarady/www/top\_story.htm > . The numerical IP address is "salticus-peckhamae.mit.edu." Moral: any URL containing the "@" sign should be parsed carefully to find out where it is \_really\_ pointing. Warnock concluded, "The RISK is that users are being bombarded with these monstrosities so often that they've grown used to it, and that they'll fail to recognize when they're being sent someplace they might not really want to go!! (Perhaps when it's not a joke, such as being sent to a porn site while working at a company with a "no tolerance" policy.)"





# 26.7 SWDR (Software-defined radio)

2000-12-07 **Keywords:** software-defined radio vulnerability

NewsScan (reprinted with permission), San Jose Mercury News < http://www.mercurycenter.com/svtech/news/breaking/merc/docs/071981.htm >

#### Vol #

Called "software-defined radio," an emerging technology allow wireless devices to download new software to add capabilities or perform different functions, thereby enabling a single product to switch, for example, from serving as a cell phone to receiving FM radio broadcasts or providing Internet access -- all without requiring new hardware. Seeing this innovation as offering a better way of managing the nation's airwaves, the Federal Communications Commission is developing new rules for approving equipment that can be altered. The technology makes it possible to switch the part of the airwaves on which the gadget can operate and seek out less crowded frequencies that are not being used. (AP/San Jose Mercury News 7 Dec 2000)





# **26.8** MAC OS

2000-01-03 **Keywords:** operating system patch DDoS distributed denial of service SecurityPortal.com (reprinted with permission), ZDNet < http://macweek.zdnet.com/1999/12/26/dosbug.html >

#### Vol #

Apple . . . released a patch for Mac OS 9's Open Transport networking protocol to correct a "flaw" that leaves Macs vulnerable to hackers who could enlist the computers over an Internet connection in distributed denial-of-service attacks without the users' knowledge.





# 27 Tools for evaluating vulnerabilities

2000-02-21 **Keywords:** QA quality assurance source code scanner database

RISKS, < http://www.rstcorp.com/its4/ >

**Vol** 20 # 81

John Viega announced release of an open-source vulnerability scanner for C and C++ source code. ITS4 uses a database of vulnerabilities and is open to refinements by its users to identify increasingly subtle security flaws in code. The Web site described the product as follows:

"ITS4 Software Security Tool

The Software Security Group at Cigital designs, analyzes and tests security-critical software. We developed ITS4 to help automate source code review for security. ITS4 is a simple tool that statically scans C and C++ source code for potential security vulnerabilities. It is a command-line tool that works across Unix and Windows platforms.

ITS4 scans source code, looking for function calls that are potentially dangerous. For some calls, ITS4 tries to perform some code analysis to determine how risky the call is. In each case, ITS4 provides a problem report, including a short description of the potential problem and suggestions on how to fix the code.

ITS4 and its source code are provided here to the security community for any use that does not compete with Cigital's consulting practice."





# 28.1 DoS attacks

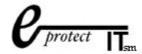
2000-07-03 **Keywords:** criminal hacking denial of service DoS telemetry RISKS, BBC

**Vol** 20 # 93

Peter G. Neumann wrote, "According to the BBC, 3 Jul 2000, a computer hacker endangered shuttle astronauts in 1997 by overloading NASA's communication system after tapping into the NASA system monitoring the astronauts' on-board medical signs while docking with Mir. Apparently, NASA has experienced more than 500,000 cyber attacks in the past year."

In a quick riposte from an alert RISKS reader, the story was debunked by a terse denial from officials at NASA HQ and the Johnson Space Center: "News reports that a computer hacker endangered the lives of Space Shuttle astronauts during a 1997 mission are wrong." Seems there was a brief interruption of medical telemetry by a hacker but no significant effects.





2000-12-10 **Keywords:** spam unsolicited commercial bulk e-mail UCE denial-of-service attack DoS delay availability bandwidth saturation

RISKS, InformationWeek < http://www.informationweek.com/817/verizon.htm>

**Vol** 21 # 15

In December, 70,000 Verizon ISP customers were significantly slowed (up to several hours) in their access to the Net because of three denial-of-service attacks within two weeks involving millions of unsolicited commercial e-mail ("spam"). Or at least, that's what Verizon \_claimed\_; however, Steve Wildstrom wrote to RISKS expressing skepticism: "Interestingly, Verizon has failed to come up, at least in public, with any evidence that this was in fact an attack. Given the company's dubious service record, a lot of folks suspect this may be a pretty lame attempt to blame a popular bogeyman for an inability to handle traffic. . . . An attack would almost certainly have involved a large number of messages from a small number of sources and at least the mail relays that the messages were sent through would have been identifiable, if not the ultimate source."





# 28.2 DDoS attacks

2000-02-07 **Keywords:** Web site attack coordinated distributed denial of service attack connectivity failure outage

Wired < http://www.wired.com/news/print/0,1294,34178,00.html>; CNet News

Vol #

On Monday the 7th of February 2000, a distributed denial-of-service attack starting around 10:15 PST prevented access to the popular Yahoo site. According to the spokesperson for Yahoo's main hosting service, "The Global Center network is not down. There've been no fiber cuts... This is a specific attack on Yahoo by external forces. This affected accessibility to Yahoo, [which] hosts servers for its site at Global Center." In following days, similar attacks disabled eBay, Amazon.com, Buy.com and CNN.com sites.

2000-02-08 **Keywords:** distributed denial-of-service attack tools Internet Web download law enforcement investigation

CNET news.com < http://news.cnet.com/category/0-1005-200-1545456.html >

Vol #

Evan Hansen and John Borland of CNET news.com summarized the key issues in the distributed denial-of-service (DDoS) attacks affecting the Web in early February 2000. Trinoo, Tribe Flood Network and Stacheldraht programs use client software illegally installed on poorly-secured systems to amplify commands for coordinated, high-volume bombardment of specific victim sites. Paul Tharp wrote a clear summary of the problem for the New York Post pointing out that the roots of the DDoS lie far back in the development of the Internet — an environment where trust was the norm and a ping (request for information) was never perceived as a threat.





2000-02-10 **Keywords:** distributed denial-of-service attacks DDoS perpetrators authors criminal hackers bragging vandalism hactivists

ZDNet News < http://news.excite.com/news/zd/000210/17/hunting-web-attackers >

Vol #

Robert Lemos of ZDNet News reported on the hunt for the perpetrators of the wave of distributed denial-of-service attacks (DDoS) that slowed access to some high-profile sites in February 2000. Criminal hackers such as "Mixter," allegedly the author of the Tribe Flood Network used in DDoS attacks, commented that tracking the attacks is extremely difficult, especially since the backtracking would be likely to find the compromised machines on which slave programs had illegally been implanted by the criminals. One slim hope for finding the perpetrators was bragging; however, several unlikely claims had already been floated by disturbed individuals such as someone calling himself "Captain Zap" who issued an 18-page manifesto claiming responsibility for the attacks and by newly-minted alleged collectivities such as the "Sovereign Anarchist Internet Militia."

2000-02-15 **Keywords:** denial-of-service attacks costs consequences estimates

NewsScan (reprinted with permission), TechWeb < http://www.techweb.com/wire/story/TWB20000214S0006>

Vol #

The Yankee Group [reported] that losses attributable to last week's denial-of-service attacks on major U.S. Web sites could total more than \$1.2 billion. The research firm says the attacks resulted in capitalization losses that exceeded \$1 billion on the days of the attacks and losses in advertising and sales on those days are expected to exceed \$100 million. The report calls for Web sites to beef up their security, and patch holes and vulnerabilities in their systems. It predicts that affected Web sites and their peers will spend an additional \$100 million to \$200 million on these upgrades. (InformationWeek 14 Feb 2000)





2000-02-17 **Keywords:** denial-of-service attacks investigation law enforcement police ISP OTC Newsbytes

Vol #

The RCMP was investigating the identity of a teenaged criminal hacker calling himself "mafiaboy" who was thought to be one of the perpetrators of the massive distributed denial-of-service (DDoS) attacks on major Web sites in early February. The Canadian federal police were cooperating with the FBI after theLook Communication ISP in Montreal turned over records to help track down the suspect. Security experts warned, however, that copycats were using the same pseudonym as a result of publicity following the DDoS attacks.

2000-02-17 **Keywords:** law enforcement investigation criminal vandal denial of service NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/business/A59099-2000Feb16.html>

Vol #

Federal Bureau of Investigation director Louis J. Freeh [said] his agency is pursuing "fast-developing leads" to hunt down the vandals who recently made a number of denial-of-service attacks on leading Web sites, and Attorney General Janet Reno is asking Congress for an additional \$38 million to fight computer crime by training local police and prosecutors, hiring 100 new FBI computer analysts, and adding 68 lawyers to prosecute computer crimes. Freeh believes that the FBI has gotten excellent cooperation from businesses targeted by the attacks, but security expert Mark Rasch of Global Integrity Corp. says that companies have expressed fear that FBI inquiries will disrupt their business operations: "One of the problems you have is fundamental mistrust between the private sector and the law enforcement community. They're afraid of losing control of the investigation. They are concerned the FBI will ask what computer was hit . . . and walk away with your main server." (Washington Post 17 Feb 2000)





2000-02-22 **Keywords:** DDoS distributed denial-of-service attacks analysis sociology fundamentals community

Red Rock Eater News

Vol #

Prof. Phil Agre, owner of the Red Rock Eater News, published a cogent analysis of the distributed denial-of-service (DDoS) attacks that shook the world of e-commerce in early February 2000. Agre said that the fundamental structure of the Internet combined with widespread ignorance by normal users of unsecured computers contributed to the vulnerability of the systems. He predicted that there would be enormous pressure against unsecured sites being used as platforms for the DDoS attacks.





2000-02-22 **Keywords:** distributed denial-of-service attacks DDoS vigilantes corporations information secrets sharing government policy

New Thinking

Vol #

Gerry McGovern, President of the Irish I.T. consulting company NUA, wrote in his weekly \_New Thinking\_ column that he was worried about news that US banks were warned about impending distributed denial-of-service (DDoS) attacks but kept the information to a tightly-knit group of financial institutions rather than sharing it with the public and security organizations. He argued that this behavior, as well as being counter-productive in the long run, was anti-social. He accused big business of usurping some of the rights and responsibilities of governments and ended, "Government has flaws; we all know that. But government is our best attempt to create institutions that allow society to be managed in a civilised manner. Without government the choice is chaos or vigilantism. The current search for the hackers behind the major spate of website attacks is a mix of both. Scores of security firms are out looking for the culprits. Their driving objective has nothing to do with law and justice and everything to do with the hoped for PR announcement that their firm caught the nasty hacker. Members of these firms are posing as suspects and friends of suspects in online chat rooms and other areas, to the extent that 'suspects' are turning up all over the place at the same time confusing everybody. . . . Law enforcement on the Internet is becoming a farce, and that's not good for anybody. Internet business will suffer if consumer confidence in the medium declines. As much as we would all like to clean up politics and make government more accountable, today right now - it is still all we've got. I have no problem with big business per se, but I don't want it 'protecting' my privacy and I don't ever want it out 'policing' my streets".





2000-05-01 **Keywords:** criminal hacker tools software denial of service NewsScan (reprinted with permission)

Vol #

Like legitimate software developers, who issue progressively improved versions of their applications, crackers seem to have released an early version of a powerful new tool that attacks and brings down Web sites. The new tool, "Mstream," which is made to launch "distributed denial of service" attacks, is similar to the ones that hosed up Yahoo and other Web sites earlier this year. In a denial of service attack, programmers embed software into hundreds or thousands of computers. Later, on cue, those computers send messages to a targeted server. The volume of Internet messages knocks out the target, rendering it inaccessible to other users. Mstream's core attack engine appears to be more potent than earlier versions and it may be able to carry out its nefarious task with only a handful of computers. Further, it can also damage the network of attacking host computers by overburdening those systems with a protective technique called "egress filtering," in which the hosts try to discard the packets they send. (New York Times 1 May 2000)

2000-05-26 **Keywords:** denial of service DoS Web attack

**RISKS** 

**Vol** 20 #

The National Hockey League was down for five days in late May due to a distributed denial-of-service attack.





2000-06-09 **Keywords:** Trojan denial-of-service attacks zombie slave platform

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB960516256118849978.htm>

Vol #

Network Security Technologies Inc. has warned the FBI that a new "attack" . . . [Trojan] has already been implanted on as many as 2,000 computers worldwide, and could be used to cripple e-commerce and other Web sites. The company discovered the virus, which is hidden in a small video file received in e-mail or found on the Net, when an employee inadvertently downloaded and launched the program. The software can turn a victim's computer into a platform for remote-controlled "denial-of-service" attacks on Web sites. The program is disguised as a video file in the so-called avi format, but actually includes an "exe" extension, which launches the virus. Network Security officials say they've identified two computers and their owners -- one in Maine and one in Canada -- who appear to be implicated in the plot. (Wall Street Journal 9 Jun 2000)





# 28.3 DoS countermeasures

2000-02-14 **Keywords:** denial-of-service attacks investigation law enforcement LEO police NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/business/A51397-2000Feb14.html>

### Vol #

Based on information provided to it by two computer experts, David Brumley of Stanford University and Joel de la Garza of the security firm Securify.com, the FBI [was] preparing to question two hackers nicknamed "Coolio" and "Mafiaboy" to determine whether they were responsible for recent denial-of-service attacks against such major Internet companies as Yahoo, Amazon. Buy.com, eBay, and CNN.com. Another security expert, Michael Lyle, says that Mafiaboy showed up last week on chat groups frequented by hackers and adds: "We entered into a number of conversations with Mafiaboy and we saw him asking for suggestions on what sites to attack and after someone would suggest a site, that site would go down." (Washington Post 15 Feb 2000)

2000-02-18 **Keywords:** DDoS distributed denial-of-service attacks colloquium discussion university

Stanford University Computer Systems Laboratory

#### Vol #

On 2000-02-23, the Stanford University Computer Systems Laboratory held a colloquium on the recent distributed denial-of-service (DDoS) attacks on Internet sites. Participants included David Brumley, Assistant Computer Security Officer for Stanford University; Joel de la Garza, security consultant for Securify; and Mark Seiden, Director of Securify Labs and Practice Area Head for Physical Security.





2000-02-19 **Keywords:** DDoS distributed denial-of-service attacks White House meeting government policy President

Prof. Gene Spafford / CERIAS — Purdue University

#### Vol #

Prof. Gene Spafford attended an emergency meeting at the White House on Friday 2000-02-11 to discuss the distributed denial-of-service (DDoS) attacks on major Internet sites that occurred at the beginning of February. He summarized the main points from the discussion as follows (quoting directly):

- 1) The Internet is international in scope, and most of the companies present have international operations. Thus, we must continue to think globally. US laws and policies won't be enough to address all our problems.
- 2) Privacy is a big concern for individuals and companies alike. Security concerns should not result in new rules or mechanisms that result in significant losses of privacy.
- 3) Good administration and security hygiene are critical. The problems of the previous week were caused by many sites (including, allegedly, some government sites) being compromised because they were not maintained and monitored. This, more than any perceived weakness in the Internet, led to the denial of service.
- 4) There is a great deal of research that yet needs to be done.
- 5) There are not enough trained personnel to deal with all our security needs.
- 6) Government needs to set a good example for everyone else, by using good security, employing standard security tools, installing patches, and otherwise practicing good INFOSEC.
- 7) Rather than new structure or regulation, broadly-based cooperation and information sharing is the near-term approach best suited to solving these kinds of problems.





2000-02-25 **Keywords:** criminal hacker distributed denial-of-service attacks

**CNN** 

Vol #

At the end of February, FBI investigators and private security firms continued their search for the perpetrators of the extensive distributed denial-of-service attacks on major Web sites at the start of the month. The investigators were using log files from the affected systems and some of the slave-program-infested sites that were remotecontrolled to send the flood of spurious requests to the victims. Some of the router logs show they were swamped with ore than 1 Gb/second of data during the attacks — and it was very important that the routers were the specific targets, since it made defensive measures all but impossible in real time. Some of those slave-infested computers included systems at Stanford University, UCLA, the University of California at Santa Barbara, and home business computers in Oregon. Logs from the #Goonies channel on IRC show someone calling itself "Coolio" (of which there are many, including one in the GlobalHell criminal hacker gang and one that claimed credit for defacing Web sites of DARE (the anti-drug program) and the US Commerce Department's Chemical Weapons Convention site in November 1999. Coolio boasted on IRC about hacking Amazon, the Russian Trek Travel site; it appears the boasting identified the precise time of the attack, something that had not yet been published by the news media. The number of tips, including some from the computer underground, was very high and every field office in the US had agents hunting down the leads.





2000-04-19 **Keywords:** denial-of-service attacks criminal hacker juvenile investigation arrest NewsScan (reprinted with permission), MSNBC < http://www.msnbc.com/news/396994.asp>

Vol #

A 15-year-old Canadian boy . . . [was] arrested in connection with the denial-of-service attacks that crippled major Web sites including Yahoo, CNN.com, eBay and Amazon in February. The Montreal-area teenager, who uses "Mafiaboy" as his online moniker, was fingered after investigators were able to trace the attacks to that name by examining the log files of a computer at the University of California-Santa Barbara, one of the servers used in the cyber-assaults. (AP/MSNBC 19 Apr 2000)





# 29 Peer-to-peer networking





2000-02-18 **Keywords:** peer-to-peer networking risks

KTSL < http://www.ktsi.net/whsecurityp2p.html>

**Vol** 20 # 76

"Security Concerns for Peer-to-Peer Software" by Mike Petruzzi < mpetruzzi@ktsi.com> , Rob Sherwood, John Dunnivan, Rob Chavez and Pat Holley of Key Technologies and Security, Inc. reviews the security implications of programs such as Napster, Gnutella and their possible variants.

The following extracts (slightly reordered) from their well-written paper are reprinted with the kind permission of my old friend and colleague, Fred Tompkins, Senior Vice President of KTSI.

Peer-to-peer (hereafter referred to as P2P) communication software allows individual computers to share and swap various types of files. Recently, P2P software has been much in the news due to current and potential lawsuits. Napster, the company that makes software for exchanging MP3s (encoded music files), is being sued for copyright infringement; the recently re-released Gnutella has the potential for exchanging all types of files and may therefore be embroiled in litigation even more quickly than Napster was.

P2P software takes the idea that the Internet is for sharing to new levels. P2P has been described as "an anarchistic threat to the current Internet" (David Streitfeld, The Washington Post, July 18, 2000) and Marc Andreesen has called P2P software the most important thing on the Internet in the last six years (when Netscape was first released) and a "benevolent virus." Ian Clarke, the creator of FreeNet, says, "People should be free to distribute information without restrictions of any form."

Even protected code is not safe. Programs like AOL Instant Messenger, or any other P2P software, can be reverse engineered and released as Open Source software. These programs can then be released for any operating system platform. This also gives malicious hackers the ability to change the software code so that it can be used for other purposes. This requires a great deal of programming knowledge and skill, but can still be done.

The first obvious concern is the liability of copyright infringement. Even though all of the companies that produce and release P2P software issue warnings regarding the illegalities of downloading copyrighted materials, simply releasing the software makes those illegal acts possible. Some P2P software contains security warnings





during the installation of the software and enables default settings to protect the naïve consumer and their computer. But armed with some simple knowledge of the Internet and its protocols, even a beginner criminal hacker can cause many security risks to users of this class of software.

More important than any copyright concerns are the potential security concerns for corporations and consumers. For corporations, P2P software threatens:

- bandwidth consumption
- liabilities and acceptable use violations
- undermining of security policies
- Trojan Horse and virus distribution
- disclosure of IP and MAC addresses
- telecommuters.

For individual consumers, P2P software represents:

- disclosure of IP and MAC addresses
- disclosure of connection speed
- file sharing
- Trojan horse and virus distribution.

I hope that readers will go to the KTSI Web site and read the entire article for themselves. The URL is < http://www.ktsi.net/whsecurityp2p.html > .





2000-03-07 **Keywords:** intellectual property copyright theft customer relations hostility generation gap

NewsScan (reprinted with permission), New York Times < http://www.nytimes.com/library/tech/00/03/biztech/articles/07net.html>

#### Vol #

The popular Napster software, which enables users to find and copy a wide array of digitized songs as well as share collections with others, is changing the way younger people think about copyrighted music as intellectual property, and the industry fears things may never be the same again. "There's an incredible disconnect out there between what is normal behavior in the physical world versus the online world," says Carey Sherman, general counsel for the Recording Industry Association of America. "There are people who think nothing of downloading entire CD collections on Napster who wouldn't dream of shoplifting from Tower Records. There's just a massive education program that's needed here for people to understand what goes into the creation of music." The RIAA has filed a lawsuit against Napster, which argues that it is not liable for music piracy because it doesn't keep any of the pirated files on its own servers. But punishing the individual consumer is a losing proposition: "One of the fastest ways to turn potential customers off is to say they're all a bunch of thieves," says a copyright expert at UC-Berkeley. "You start hating your customers and your customers are going to start hating you back, and that doesn't bode well for your ability to attract them to buy more stuff from you. It makes them more inclined to infringe rather than buy." (New York Times 7 Mar 2000)

Colleges and universities are split on "the Napster issue." Some are blocking Napster, some are not. Among the ones that are not are Georgia Tech, Michigan, Stanford, Duke, and the University of California at Berkeley. A Georgia Tech official says: "We are an educational institution and we will err on the side of unfettered access to information. Once you start down that road ... well, we could tie up an awful lot of staff people and resources trying to evaluate Web sites' content, and we don't want to get into that." Among the ones that are blocking Napster are Yale, Indiana, Southern California, Texas, Ohio State, Northeastern, and Canisius. The first three in this group made their decisions after being sued by two rock groups and the Recording Industry Association of America; the second two chose to block Napster on the grounds that Napster traffic clogged their computer networks; and the last two cited legal and ethical reasons for rejecting Napster and similar programs. A Canisius official explained: "It's not free for you to steal books from the public library, and it's not free to download music you haven't paid for." (AP/San Jose Mercury News 1 Oct 2000)





2000-03-24 **Keywords:** peer-to-peer networking file exchange

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/2000324/t000027817.html>

#### Vol #

Some enterprising computer hackers have come up with a variation on Napster software that helps people search and swap any type of computer file -- not just MP3 music files. The variation, dubbed "Wrapster," uses Napster's servers to exchange everything from games and movies to software and spreadsheets by tricking them into thinking the files are in the MP3 format. Napster holds patents on some components of its technology and the company's VP of engineering says it hasn't decided "whether we're going to turn a blind eye to it or actively try to disable it." Napster is currently developing its own systems that would enable other types of files to be traded. (Los Angeles Times 24 Mar 2000)

2000-04-25 **Keywords:** intellectual property copyright violations theft peer-to-peer lawsuit litigation

NewsScan (reprinted with permission), CNet < http://news.cnet.com/news/0-1005-200-1760313.html>

#### Vol #

Rap artist Dr. Dre . . . joined Metallica and the Recording Industry Association of America in suing Napster, whose controversial software, they charge, is responsible for massive copyright violations, primarily by college students who swap tunes using MP3 files. But in a new twist, Dr. Dre's lawsuit targets individual students as well as universities that permit the software to be used on their servers. No individual students or universities are named in the suit filed yesterday, but experts say it's serving as a kind of placeholder, and that five schools and students will be named later. Already, the three universities cited in the Metallica suit have blocked or sharply restricted the use of Napster on their campuses. (News.com 25 Apr 2000)





2000-04-25 **Keywords:** intellectual property copyright theft violations marketing publicity ecommerce peer-to-peer

NewsScan (reprinted with permission)

#### Vol #

Criticizing fellow rock artists and who have attacked Napster Inc. for promoting music piracy by allowing people trade and search for files of musical performances downloaded via the Internet and without remunerating artists or record companies, the lead singer of the rock band Limp Bizkit . . . [called] Napster software "an amazing way to market and promote music" and . . . [maintained] that "the Internet is here, anybody trying to fight that, which would be people who are living by certain standards and practices of the record industry ... are the only people who are scared and threatened." The Recording Industry Association of America is suing Napster for piracy and copyright infringement, as is the band Metallica. (Reuters/San Jose Mercury News 25 Apr 2000)

2000-05-09 **Keywords:** intellectual property copyright violation theft lawsuit ruling NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000509/t000043641.html>

#### Vol #

The Recording Industry Association of America claimed initial victory in its lawsuit against Napster after U.S. District Court Judge Marilyn Patel rejected Napster's argument that it is a "mere conduit" for pirated music files. The RIAA is hoping for a repeat performance of its recent win over MP3.com. A federal judge in that case ruled that MP3.com violated copyright law with its database that allows users to store music and then access it from any computer connected to the Internet. The RIAA is seeking statutory damages ranging from \$500 to \$100,000 per sound recording downloaded using Napster's software. Analysts estimated the total could approach hundreds of billions of dollars. (Reuters/Los Angeles Times 9 May 2000)





2000-05-30 **Keywords:** intellectual property copyright infringement violation NewsScan (reprinted with permission), < http://www.usatoday.com/life/cyber/tech/cth987.htm>

Vol #

Conceptually similar to Napster, the Net software company that makes it easy for users to download and trade copies of songs (either with or without permission of the copyright owners), new sites such as Scour and iMesh have developed software that allows the swapping of photos and videos as well as music. As a result, bootlegged copies of some brand new movies, including the popular "Gladiator," are available free to people willing to spend the time to download them, and willing to ignore copyright laws. Both Scour and iMesh insist they post strict legal notices and they are legitimate entertainment sites, offering authorized "trailers" (movie previews) by arrangement with movie studios such as Miramax. (USA Today 30 May 2000)





2000-06-05 **Keywords:** music sharing intellectual property copyright permission legal authorized fair use streaming

NewsScan (reprinted with permission)

Vol #

Pointera, a Palo Alto-based startup that launches today, says its service is unique in that it enables portals and users to share files, including digital music files, legally through a standard Web browser. The service is conceptually similar to Napster and Gnutella, but rather than copying the desired files, the user "shares" the file, which remains on the original computer. "We enable the streaming of media files as opposed to people just downloading," says CEO Manish Vij. "What this means is you can just hit play from your hard disk instead of hitting copy. If you're simply playing that's the same as going to someone's house and watching a movie and is still covered by fair use under the copyright laws." The Pointera Search Engine enables portal servers to work directly with individual PCs for file-sharing. "The real issue here is that the technology essentially moves beyond MP3," says Gartner Group's Chris Le Tocq. "The Pointera technology is a business application, which we've never had before. Groups of people can exchange files and work together... The interesting thing here is that this an instant process, it allows for peer to peer architecture. This is very different than the hierarchical architecture found on the Web today." (Internet.com 5 Jun 2000)





2000-06-14 **Keywords:** intellectual property peer-to-peer distribution encryption

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/library/tech/00/06/biztech/articles/14movie.htm>

Vol #

The digital video and music distribution company Sightsound.com is going to use the Gnutella software to transmit movies over the Internet as encrypted files. Giga Information group analyst Rob Enderle says, "We believe that these kinds of distribution schemes will become increasingly common as the music and movie industries realize the kind of threat they are under. SightSound executives are not commenting on the plan because the company is in a "quiet period" before an initial public offering. With Gnutella, the various files shared are stored locally on individual users' machines. The company has said it will use commercially available encryption technology to protect its content. (New York Times 14 Jun 2000





2000-06-16 **Keywords:** intellectual property music theft trafficking lawsuit litigation

NewsScan (reprinted with permission), San Jose Mercury News

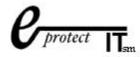
- < http://www.sjmercury.com/svtech/news/breaking/ap/docs/91264l.htm>, New York Times
- < http://partners.nytimes.com/library/tech/00/06/biztech/articles/16music.htm>

#### Vol #

[In June,] The Recording Industry Association of America . . . asked a federal judge to grant an injunction preventing Napster, the online service that allows individuals to swap music collections without necessarily observing copyright laws, from "facilitating or assisting others in, the copying, downloading, uploading, transmission or distribution of copyrighted musical works." The request was supported by the Motion Picture Association of America and by MP3.com. MPAA president Jack Valenti . . . [said]: "If Napster can encourage and facilitate the distribution of pirated sound recordings, then what's to stop it from doing the same to movies, software, books, magazines, newspapers, television, photographs or video games?" (AP/San Jose Mercury News 13 Jun 2000)

Defending itself against a copyright lawsuit against the Recording Industry Association of America for making it possible for over 10 million computers users to share copyrighted files, the Internet music distribution company Napster.com . . . [said in June] that it should not be sued just because it is operating on a large scale. Napster's position is that the RIAA would never sue a single individual for copying a song or movie and giving it to a friend, and so it should not be suing Napster just for facilitating such behavior on a large scale. Without conceding that it is lawful for users to share music one-on-one, the recording industry . . . [said] that "there can be no question it is unlawful when done on a large scale, as with Napster." (New York Times 16 Jun 2000)





2000-07-12 **Keywords:** wireless communication Internet access e-mail peer-to-peer networking NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/library/tech/00/07/biztech/articles/12cybiko.html>

Vol #

Seeing "a huge opportunity with 12-16 year olds," the New York start-up company Cybiko is marketing a \$129 device with an LCD screen, small keyboard, and the ability to communicate with similar devices within 300 feet. If one device within that range is connected to an Internet-connected PC, other Cybikos can send and receive e-mail, and if the devices are equipped with optional digital music players they will be able to share music downloaded from the Internet as MP3 files. Cybiko's president said, "We want to create a social environment where teens can chat and interact." (AP/New York Times 12 Jul 2000)

[Comment by MK: This P2P technology offers considerable scope for breaches of security. On the face of it, schools and universities will have to ban such devices from examinations much as Palm Pilot and other devices that can exchange information via infrared frequencies have been banned. In addition, the prospect of having wireless access to Internet e-mail should prompt careful examination of potential confidentiality and forgery issues involving such devices.]





2000-07-27 **Keywords:** intellectual property IP peer-to-peer lawsuit injunction

NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/articles/A50239-2000Jul26.html>

#### Vol #

A federal judge in San Francisco . . . issued a preliminary injunction ordering Napster.com, which provides free software allowing music-lovers to swap files of music downloaded from the Internet, to shut down its operations. Dismissing arguments that Napster users were merely exercising their First Amendment rights, U.S. District Judge Marilyn Hall Patel concluded that the illegal duplication of copyrighted material "was the whole reason for Napster's existence." The judge hinted that the Recording Industry Association of America, the plaintiffs in the suit, would ultimately prevail against Napster in a full-blown trial: "I find the plaintiffs have established not only a reasonable likelihood of success, but have shown a strong likelihood of success on the merits." (Washington Post 27 Jul 2000)

2000-07-31 **Keywords:** intellectual property IP copyright infringement lawsuit negotiation settlement

NewsScan (reprinted with permission)

#### Vol #

Though Napster chief executive Hank Barry . . . [suggested there was] an opportunity to reach an out-of-court settlement in the copyright infringement suit brought against his company by the Recording Industry Association of America (RIAA), one recording company executive . . . [scoffed]: "Napster doesn't even have a business plan. There's really nothing they could offer us in settlement talks except a mailing list of people who want free music." But other record executives think some kind of settlement is inevitable, and one of them explains: "Nobody thinks the technology is going away. The point is to win the suit and keep the venture capitalists away from it." (Reuters/San Jose Mercury News 31 Jul 2000)





2000-08-21 **Keywords:** peer-to-peer intellectual property IP culture sociology psychology NewsScan (reprinted with permission)

Vol #

A report from scientists at the Xerox Palo Alto Research Center who studied the Gnutella system, which people can use to "share" music downloaded from the Internet, . . . [said] most users are takers but not givers. See < http://www.parc.xerox.com/istl/groups/iea/papers/gnutella> . The scientists call the lack of true sharing "a tragedy of the digital commons." (New York Times 21 Aug 2000)





# 2A Firewalls & other perimeter defenses

 $2000 \hbox{-} 02 \hbox{-} 26 \qquad \textbf{Keywords:} \qquad \text{cable modem home PC workstation criminal hackers vulnerability}$ 

tunneling corporate systems compromise passwords dialup

Australian

Vol #

Security expert Christopher Rouland of Internet Security Systems (ISS) warned that cable-modem users are at risk of attack by criminal hackers because of the users' full-time presence on the Net. He urged users to protect their PCs against penetration and warned against tunneling to their corporate systems when using cable modems. Hackers who penetrate unprotected cable-modem users' systems could steal dialup IDs and passwords stored on the local computers, he said.





2000-08-13 **Keywords:** firewall vulnerabilities exploits demonstration conference RISKS, ZDNet < http://www.zdnet.com/zdnn/stories/news/0,4586,2610719,00.html > **Vol** 21 # 02

A demonstration at the Black Hat security conference in Las Vegas showed how the Checkpoint Firewall-1 could easily be defeated by hackers. The successful attacks included

- \* impersonation of an authorized admin;
- \* making a non-secured Internet connection look like an authorized VPN connection;
- \* exploiting filtering algorithm errors to pass dangerous commands through the firewall.

The panelists warned that their demonstration was not specific to the Checkpoint product but applied to other products as well. The Director of Product Marketing for Checkpoint warned that the exploits depended on bad configuration of the devices. Fixes for the vulnerabilities were issued with the cooperation of the three lecturers (John McDonald and Thomas Lopatic of Data Protect GmbH plus Dug Song of U. Michigan).





# 2C Addiction, cyber-syndromes, sociology

2000-03-01 **Keywords:** cybersex addiction syndrome habit

NewsScan (reprinted with permission), New York Times < http://www.nytimes.com/aponline/a/AP-Online-Sex.html>

#### Vol #

Psychologists from Stanford and Duquesne universities have published an article in the journal Sexual Addiction and Compulsivity claiming that at least 100,000 users are cybersex compulsives who spend more than 11 hours a week visiting X-rated Web sites and chat rooms. The study concludes: "This is a hidden public health hazard exploding, in part, because very few are recognizing it as such or taking it seriously." The researchers believe that cybersex compulsives have difficulty maintaining normal relationships with others. (AP/New York Times 1 Mar 2000)





2000-09-19 **Keywords:** allergy toxic computer equipment plastic contamination

NewsScan (reprinted with permission), TechServer

< http://www.techserver.com/noframes/story/0,2294,500259402-500399748-502393843-0,00.html>

Vol #

Chemicals from computer screens can provoke allergies, according to a Swedish study published . . . [18 Sep] in the journal Environmental Science and Technology. Researchers from Stockholm University say the chemical compound triphenyl phosphate, a flame retardant widely used in the plastic of video monitors and computers, can cause allergic reactions such as itching, nasal congestion and headaches. The problem arises when the temperature of the screen or video monitor begins to rise, says the study's lead author. "We have focused our interest on this compound since it has been proven to be a contact allergen to man and due to the fact that a number of workers in Sweden have acquired health problems related to computer work." Significant levels of the compound were found in more than half of the 18 computer brands tested by researchers, who recommend lots of ventilation to alleviate the problem. (Agence France Presse/Nando Times 19 Sep 2000)





2000-10-02 **Keywords:** socioeconomic factors digital divide availability bandwidth access knowledge skills

NewsScan (reprinted with permission)

Vol #

As many as 50 million U.S. adults are at risk for becoming functionally illiterate in the coming years because they're technologically deprived, according to a Gartner Group study. "The Internet will soon be so pervasive that not having access to the technology or not knowing how to use it will be the equivalent of not knowing how to read or write," . . . [said] Gartner CEO Michael Fleisher. The report confirms the existence of a "digital divide" that denies 65% of "lower socioeconomic-status" Americans access to the Internet, compared with only 17% in the top income bracket. But beyond simple access, a second "experience gap" separates people knowledgeable enough to tap the benefits of the Internet from those who are not. Meanwhile, a third divide is developing between those with high-speed, broadband access and those stuck with straight dialup accounts. "As broadband access reaches higher penetration rates, we can expect to see a gap in broadband adoption that mirrors today's gaps in (personal computer) ownership. This will be the equivalent of having the moderate and upper classes in IMAX theaters while the underprivileged are still watching silent movies," says Fleisher. (Reuters/MSNBC 2 Oct 2000)





## 2D Port scanning

2000-10-17 **Keywords:** worm penetration port scan infection counterattack response revenge retaliation infection

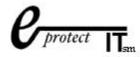
**RISKS** 

**Vol** 21 # 09

A correspondent called "Jeremy" noted in RISKS that the number of netbios probes went up by an order of magnitude in September and October. He pointed out that these systems are presumably infected with a worm or virus and are doing the bidding of the malware writers; however, the infected systems are also announcing all over the Net that they have poor security. "Jeremy" postulated that there could be three types of active response to these probes by anyone interested:

- \* sterilizing the infections remotely;
- \* planting another virus or worm;
- \* disabling the infected machine.





## **2E** Voting using computers

2000-01-18 **Keywords:** internet online voting study report state government task force California State Government < http://www.ss.ca.gov/executive/ivote/ >

Vol #

The California Internet Voting Task Force issued its "Report on the Feasibility of Internet Voting." A key section from the Executive Summary: "
The implementation of Internet voting would allow increased access to the voting process for millions of potential voters who do not regularly participate in our elections. However, technological threats to the security, integrity and secrecy of Internet ballots are significant. The possibility of "Virus" and "Trojan Horse" software attacks on home and office computers used for voting is very real and, although they are preventable, could result in a number of problems ranging from a denial of service to the submission of electronically altered ballots.

Despite these challenges, it is technologically possible to utilize the Internet to develop an additional method of voting that would be at least as secure from vote-tampering as the current absentee ballot process in California. At this time, it would not be legally, practically or fiscally feasible to develop a comprehensive remote Internet voting system that would completely replace the current paper process used for voter registration, voting, and the collection of initiative, referendum and recall petition signatures."





2000-09-21 **Keywords:** online voting fraud contest TV show

RISKS, Australian Broadcast Corp. < http://www.abc.net.au/mediawatch/transcripts/s181183.htm >

**Vol** 21 # 06

The Australian Broadcasting Corporation found strong indications of voting fraud when it allowed online voting for the popularity of amateur videos on a TV show. The leading contender received five times more votes than any other contestant despite the fact that her videos were despised by the professional judges.





2000-10-20 **Keywords:** electronic voting workshop

**Vol** 21 # 10

**RISKS** 

The Internet Policy Institute (IPI) held a workshop on October 11 & 12, 2000 to examine the issues associated with conducting public elections via computer networks. Sponsored by the National Science Foundation (NSF) and chaired by C.D. Mote, Jr., president of the University of Maryland, this workshop was in response to a request by the White House to study the feasibility of Internet voting. Avi Rubin participated in the workshop and wrote in RISKS:

"Panels were held discussing issues such what e-voting means, whether or not e-voting would improve accessibility, whether it would widen the digital divide, and whether more people would vote. On the technical side, there were panels about the security requirements, the current state of security on desktops as related to voting.

The mandate was to cover the following issues:

- \* How to ensure the security and reliability of the voting process;
- \* How to protect the privacy of voters;
- \* How to authenticate voter identity;
- \* How to achieve broad and equitable access to online voting systems;
- \* How to assess the impact of online voting on representative democracy and community; and
- \* How to ensure that online voting systems are convenient, flexible, and cost-effective."





2000-10-26 **Keywords:** online voting security prediction

NewsScan (reprinted with permission), Associated Press, San Jose Mercury News < http://www.mercurycenter.com/svtech/news/breaking/ap/docs/564217l.htm >

Vol #

Concerned about issues of security, confidentiality and ease of use, election officials are being extremely cautious about letting citizens use the Internet to cast their votes: in the coming elections fewer than 200 people will be eligible to vote from their PCs. Maine secretary of state Dan Gwadosky sums up the current situation this way: "Online voting is inevitable. It just won't happen on Internet time." (AP/San Jose Mercury news 26 Oct 2000)





2000-11-07 **Keywords:** voting computers proprietary software Trojans QA quality assurance open source fraud

**RISKS** 

**Vol** 21 # 10

Douglas W. Jones, the chair of the Iowa State Board of Examiners for Voting Machines and Electronic Voting Systems, wrote an essay for RISKS in which he expressed concern over the growing use of proprietary software for voting machines and other forms of electronically-mediated voting. He pointed out that such software makes it much easier to insert Trojan code than, say, open-source software.

He ended his essay as follows: "The time has come for computer professionals to press for a change to the guidelines for voting machines, asking that all software included in such machines be either open source, available for public inspection, or at least open to inspection by a third party independent testing authority. There are no technical obstacles to this! Linux, Free BSD and several other fully functional operating systems are available and will run on the hardware currently being incorporated into modern voting machines!

But, this is not the end of the problem! How do you prove, after the fact, that the software in the voting machine is the software that was approved by the board of examiners and tested by the independent testing authority? No modern machine I'm aware of makes any real effort to allow this proof, although several vendors do promise to put a copy of their source code in the hands of an escrow agency in case a question arises".





2000-11-08 **Keywords:** online voting problems satire funny

**RISKS** 

**Vol** 21 # 11

Lauren Weinstein's "Reality Reset" < http://www.vortex.com/reality > included a hilarious satirical "interview" with "Paddy Mastoid. . . . president of trust-us-not-to-badly-screw-up-your-vote.com, a firm promoting Internet voting systems." In this spoof, Weinstein, Co-Founder of PFIR (People For Internet Responsibility, < http://www.pfir.org > ) and Moderator of the Privacy Forum < http://www.vortex.com > , ably reviews many of the vulnerabilities to hacking that online voting systems present.

2000-11-14 **Keywords:** online voting predictions

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cti797.htm >

Vol #

Some technology chief executives are predicting that Web-based voting will be in place by the time of our next presidential election, and one of them argues: "You can trade stock online. There's plenty of technology to implement Internet voting." But Jim Cannavino of the security firm CyberSafe says "I haven't seen us move fast on any of these things," and doesn't think the Internet voting will happen until 2050, because it will take that long for government leaders to understand the system well enough to believe in its validity." (USA Today 13 Nov 2000)





2000-12-12 **Keywords:** electronic voting security testing challenges contests RISKS

**Vol** 21 # 14

In a manifesto published in the IP distribution list and on the RISKS Forum, eminent computer scientists Peter Neumann (SRI), Rebecca Mercuri (Bryn Mawr), and Lauren Weinstein (PFIR, Privacy Forum) attacked the practice of putting proprietary electronic voting systems out for random attacks as a method of evaluating their level of security. "In fact, using such "tests" as any sort of validation technique runs contrary to long-established computer and engineering verification practices, and makes a mockery of the rigorous design and testing that is required of systems that are to be deemed secure through extensive and methodical processes (e.g., to gain certification under the ISO Common Criteria or its predecessors TCSEC/ITSEC)."

2000-12-13 **Keywords:** online voting

RISKS

**Vol** 21 # 15

Fred Cohen analyzed the security issues in online voting in a paper published in the RISKS Forum. Having listed ten necessary properties for a trustable election process, he noted, "At this point in time, and for the foreseeable future, computerized and particularly Internet-based voting machines and networked voting systems do not, and will not, fulfill the majority of these requirements." He went on to list ten specific objections to online voting systems in today's technical environment.





2000-12-15 **Keywords:** online voting research study project

NewsScan (reprinted with permission), San Jose Mercury News < http://www.mercurycenter.com/svtech/news/breaking/merc/docs/010800.htm >

#### Vol #

[In December, a] team of political scientists, engineers, and design experts from the Massachusetts Institute of Technology and the California Institute of Technology . . .[announced that they would] undertake a study of existing voting technology and create a plan to improve it. Caltech president David Baltimore said it is "embarrassing to America when technology fails and it puts democracy to such a test as we have seen in the last month," and his counterpart MIT president Charles Vest promised that, "to a large extent, the problem that the country has ... a technological solution." (AP/San Jose Mercury News 15 Dec 2000)





2000-12-19 **Keywords:** online voting automated teller machines ATM ABM RISKS

**Vol** 21 # 15

David Jefferson wrote a thoughtful analysis of proposals for using automated teller machines (ATMs) for voting. Although such machines are often equipped with security measures, Jefferson showed major disadvantages that preclude using them for elections. In summary, his objections to using the ATM networks for voting were as follows:

- \* Private voting, like absentee balloting, is subject to voter intimidation, coercion and vote-selling;
- \* Voter authentication is problematical, since vote-sharing (voting by proxy) is illegal;
- \* Reliability of electronic voting using banking networks would be problematic;
- \* Independent oversight by election officials would be complicated if the privately-owned ATM networks were used for voting;
- \* The security of the banking networks would be equally compromised if election officials had access to financial systems;
- \* It is unthinkable that banks would turn over complete control of their systems to public officials even for a single day, let alone for the time required "to build, debug and certify such a system. . . . "

Therefore, concludes Jefferson, "the suggestion to use the ATM network for voting is a complete nonstarter."





## 2F Spyware

2000-08-28 **Keywords:** spyware unauthorized connection upload

**RISKS** 

**Vol** 21 #

Eudora v4 has three settings for functionality: full (paid), free with ads, and limited but without ads. David Sedlock noticed that the latter mode was nonetheless accessing the Eudora site using HTTP connections twice a day without any notification to (or authorization from) the user. Eudora staff dismissed the occurrence as a minor issue because the connections were "really really fast" and did not transfer any private information from the user. Sedlock, however, noted that the unwanted connections could automatically initiate a connection to his ISP, thus incurring per-call costs to him.





# 31.1 Surveys, studies, research

2000-01-19 **Keywords:** survey study statistics computer crime cybercrime

Guardian

Vol #

Internet-related credit-card fraud rose 29% in 1999, according to the British Home Office's statistics published on the Web (see

- < http://www.homeoffice.gov.uk/rds/crime statistics> and
- < http://www.digitalcentury.com/encyclo/update/crime.html> . Cybercrime growth accounted for a major part of the rise in total crime, according to Paul Wiles of the Home Office.

2000-01-27 **Keywords:** electronic survey Web privacy policy implementation lacunae holes enforcement Web commerce intrusion monitoring government future

**EPIC Alert** 

**Vol** 7 # 01

The Electronic Privacy Information Center (EPIC) released an interesting survey of the state of privacy on the Web using a sample of 100 prominent sites. The summary was depressing: "\_Surfer Beware III\_ found that few of high-traffic websites offered adequate privacy protection. In fact, not a single one of them fulfilled important elements of Fair Information Practices investigated in the survey. Fair Information Practices serve as basic guidelines for safeguarding personal information. Also alarming was the significant proportion (35 out of 100) of shopping sites that allowed profile-based advertising networks to operate. These advertising networks present a stealthy and invasive way in that third parties -- companies that display banner advertisements -- are tracking online behavior without the knowledge of the Internet user."





2000-02-18 **Keywords:** vulnerability weakness audit report management Web Internet government

AP

Vol #

A Congressional audit report by the General Administration Office included devastating criticisms of the US Environmental Protection Agency on 2000-02-17. The EPA had already shut down its public Web site for fear of penetration in the face of observations such as, "riddled with security weaknesses" and "a likely target for hackers." The investigators "found serious and pervasive problems that essentially render EPA's agencywide information security program ineffective. . . Moreover EPA cannot ensure the protection of sensitive business and financial data maintained by its larger computer systems or supported by its agency-wide network."

2000-02-22 **Keywords:** e-commerce survey

 $News Scan \ (reprinted \ with \ permission), \ CNet < http://news.cnet.com/news/0-1007-200-1554830.html>$ 

#### Vol #

A Forrester Research survey last summer [1999] of 17,000 households in Germany, France, Sweden, the Netherlands and the U.K. indicates that less than 10% of respondents were interested in shopping online. In Sweden, where e-commerce was most popular, 14% of households were connected to the Web and 7% had ordered goods. At the other end of the scale, only 7% of French households were linked to the Net, and only 2% had bought anything. However, a third of French homes subscribe to Minitel, which has offered shopping and information services for 17 years, and presents a strong challenge to Internet-based e-commerce in that country. Most respondents cited privacy concerns and the inability to actually see what they were buying as the major impediments to e-shopping. (Reuters/CNet News.com 22 Feb 2000)





2000-03-02 **Keywords:** poll survey study consumer confidence criminal hacking Web vandalism NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/business/A56622-2000Mar1.html>

#### Vol #

The Gallup polling organization [said] that the recent attacks by network vandals on prominent Web sites have left one-third of online consumers less likely to make a purchase via the Internet. The chief executive of At Plan, the online marketing consultancy that sponsored the Gallup poll, says that the attacks were "a cold dose or reality to many people... almost like the loss of innocence in first love." (Washington Post 2 Mar 2000)

2000-03-22 **Keywords:** CSI FBI annual survey computer crime costs losses trends study Reuters, CSI < http://www.gocsi.com/prelea\_000321.htm>, NewsScan, Los Angeles Times < http://www.latimes.com/business/20000322/t000027053.html>

#### Vol #

The annual CSI / FBI computer crime survey was released in March 2000. The self-selected response group included 273 organizations and 643 security practitioners in US corporations, government, finance, health-care, and academia. Total reported losses were \$265M. About 90% of the respondents experienced breaches of information security in the preceding 12 months; the top three problems were computer viruses, laptop theft and employee net abuse. However, 70% of the respondents also reported other types of breach: theft of secrets, financial fraud, outsider penetration of security perimeters, denial of service, and sabotage of data or networks. In addition, 74% acknowledged financial losses — higher than in the 1998-1999 survey. Some 59% of the respondents rated Internet connections as a more frequent point of attack than internal systems (38%). As usual, there were many other interesting questions and responses in the survey.





2000-05-25 **Keywords:** e-mail productivity appropriate use restrictions improvements education spam

NewsScan (reprinted with permission)

Vol #

Ferris Research . . . released the results of a study designed to quantify the costs and benefits of e-mail, and estimates that the overall benefit in terms of increased productivity equals about \$9,000 per employee. Rather than treading into the murky area of nonquantifiable benefits, such as improved decision-making, Ferris attempted to focus on items that delivered a tangible benefit, like time not spent on addressing snail mail envelopes, operating postage and fax machines, etc. It derived a 15% to 20% productivity improvement, with an overall increase of 326 hours per employee on the average. Ferris then attempted to quantify those hours, giving them a value of \$13,000. Then came the downside: Ferris found that employees waste on an average 115 hours dealing with nonproductive e-mail, translating to a loss of about \$4,000 per worker a year. Subtract the loss from the gain, and the result is an overall benefit of \$9,000 per employee, or a 15% productivity gain. Ferris says that rate can be raised to 20% by more actively managing company e-mail systems: discouraging personal e-mail, shortening e-mail distribution lists, and helping workers identify and trash spam. (Investor's Business Daily 25 May 2000)





2000-05-25 **Keywords:** intellectual property copyright infringements violations theft music sales NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000525/t000049387.html>

#### Vol #

A [highly controversial] study of music sales commissioned by Reciprocal Inc., a digital rights management company, shows that sales of recorded music have declined in the vicinity of college campuses in the last two years, while rising elsewhere. Music sales were up 12% during the first three months of 2000 over the same time period in 1998, but at stores within five miles of a college campus -- which account for about half of all music purchased -- sales were down 4%. Music industry officials attribute the dip to use of Napster, which has been especially popular among college students. Some colleges have banned the music downloading software from campus computer systems because heavy use was clogging their networks. (AP/Los Angeles Times 25 May 2000)

2000-06-12 **Keywords:** confidence government regulation industry pornography protection business research report survey focus groups

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/library/tech/00/06/biztech/articles/12mark.html>

#### Vol #

Focus groups held . . . [in June] by Greenberg Quinlan, a Washington public policy research firm, . . . [seemed] to indicate a shift in public attitudes about Internet regulation. Whereas two years ago people were more inclined to look to government to regulate pornography and other kinds of activities found on the Internet, they now seem to trust business rather than government. Stanley Greenberg, who directed the research project on behalf of the nonprofit Markle Foundation, says: "People didn't understand the Internet as well. They understand more now about the difficulty of regulation." (New York Times 12 Jun 2000)





2000-06-15 **Keywords:** intellectual property copyright theft survey purchase ethical downloading NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB961025291366759846.htm>

Vol #

A new survey, . . . [released in June] by the Digital Media Association, indicates that Internet users who download music to sample are likely to follow up by purchasing CDs in stores or online. The new poll contradicts the findings of previous studies that found digital music downloading via Napster made a significant dent in bricks-and-mortar music store sales, especially in areas around college campuses. This latest survey, conducted by market research firm Yankelovich Partners, says 66% of all consumers said that listening to a song online has at least once prompted them to later buy a CD or cassette featuring that song. Most people who downloaded music (92%) listened to it on their desktop computers, while 10% used a portable device and 14% used their home stereo. More than 60% of them used the Internet to get to music they couldn't find on radio. According to Media Metrix, 22.8 million people visited the top 30 Internet music sites in April, up 19% from November 1999, the most recent number available. Paid digital music downloading is expected to hit \$1.1 billion in sales by 2003, according to estimates by Forrester Research. (Wall Street Journal 15 Jun 2000)

2000-07-31 **Keywords:** survey study vulnerabilities weakness Web servers SSL public-key digital certificates

RISKS, < http://www.meer.net/~ ericm/papers/ssl\_servers.html >

Vol 21 # 02

Eric Murray published the results of a survey of Web security: "A random sample of 8081 different secure Web servers running the SSL protocol in active use on the Internet shows that 32% are dangerously weak. These weak servers either support only the flawed SSL v2 protocol, use too-small key sizes (40 bit encryption), or have expired or self-signed certificates. Data exchanges with all types of weak servers are vulnerable to attack."





2000-08-12 **Keywords:** audit study weakness security program government agency evaluation failure miserable pathetic fiasco

RISKS, < http://com-notes.house.gov/ai00215.pdf >

Vol 21 #

The General Accounting Office of the US government gave the Environmental Protection Agency a failing grade on computer security in August. The GAO described the agency's program as "Ineffective, inadequate, and riddled with weaknesses."

2000-08-21 **Keywords:** privacy cookies dishonesty Web personal information anonymity blocking encryption e-mail

NewsScan (reprinted with permission)

Vol #

A . . . study by the Pew Research Foundation finds that "There is broad-based concern about privacy being compromised [on the Net]," . . . [said] Lee Rainie, director of the study. Eighty-four percent of respondents reported they were concerned about businesses invading their privacy online, and many were frustrated by their unfamiliarity with the basic mechanics of Internet data collection. For instance, 56% of Internet users surveyed did not know what an Internet "cookie" is. The study attributes this lack of knowledge to the fact that about 35% of the 144 million people who use the Internet in the U.S. came online within the past year. Among more sophisticated Web surfers, only 5% use "anonymizing" software to hide their identities; 10% report using encryption software to protect their e-mail; 20% use a secondary e-mail address when forced to provide information on a Web site; and 25% say they have given a fake name or provided false responses on a Web site information form. (Los Angeles Times 21 Aug 2000)





# 31.2 Estimates, guesses, predictions, forecasts

2000-02-11 **Keywords:** estimates market value security industry

 $News Scan \ (reprinted \ with \ permission), \ WP < http://www.washingtonpost.com/wp-dyn/business/A37615-2000 Feb10.html>$ 

#### Vol #

[The early-February] cracker attacks have served as a wake-up call to the e-marketplace, and as a boon to security software firms that represent the best line of defense against further incidents. Online ventures have spent big to gain name recognition and build their reputations for service. But if customers can't get through, or if the security of their transactions isn't protected, they will abandon ship, and quickly. Suddenly, many e-businesses are realizing that the reputations they've carefully built can be wiped out by one intruder with an attitude. Shares of security software manufacturers surged for a second day Thursday, up as much as 36% for the week. "It's definitely a reaction to the news stories on hackers," said one analyst. "E-commerce and security go hand in hand. You can't have e-commerce without security." (Washington Post 11 Feb 2000)





2000-02-11 **Keywords:** awareness post-hoc reaction stupidity foolishness blindness obtuseness

industry commerce naive beginners incompetents incompetence risk assessment ignorance police LEO law enforcement evaluation software

NewsScan (reprinted with permission), San Jose Mercury News

< http://www.sjmercury.com/svtech/news/breaking/ap/docs/198908l.htm>

#### Vol #

Investigators struggling to find the people behind [the early-February] attacks on major Web sites note that, if nothing else, the assaults jarred people out of their complacency. Months ago, a Carnegie Mellon University team issued a warning about attacks like those that have occurred this week, but the public reacted with a collective yawn. Over New Year's weekend, the FBI posted free software on its site that would let PC owners detect if denial-of-service tools had been secretly placed on their machines. Few showed any interest. "This week's events did more than we have ever been able to do with white papers and posting fixes on our Web site to alert the private sector to the dangers out there," said a spokesman for the attorney general's office. The Clinton Administration this week sought \$37 million to set up 10 regional computer labs and train state and local officers as computer response experts. (AP/San Jose Mercury News 10 Feb 2000)

2000-03-14 **Keywords:** Internet growth

 $News Scan \ (reprinted \ with \ permission), \ Washington \ Post < http://www.washingtonpost.com/wp-dyn/articles/A2613-2000 Mar 13. html>$ 

#### Vol #

At a high-tech conference in Virginia Michael S. Dell, founder of Dell Computer, predicted that there will be 500 million Internet users by 2003 and Internet pioneer Vinton G. Cerf, now with MCI WorldCom, said that by 2006 there will be more than 900 million devices linked to the Internet, equal to the number of telephones in the world. But Dell said \$370 billion will have to spent in 2003 on new Internet infrastructure because only about 5% of network servers now in place will be usable in a few years and capable of supporting faster connections demanded by Internet users. (Washington Post 14 Mar 2000)





2000-09-11 **Keywords:** information warfare penetration industrial espionage proprietary information intellectual property IP survey study losses estimate

NewsScan (reprinted with permission), MSNBC < http://www.msnbc.com/news/457161.asp>

Vol #

Teenage hackers who deface government sites or steal credit card numbers attract a lot of attention, but experts say the real problem of cybercrime is corporate-sponsored proprietary information theft committed by professionals who rarely get caught. According to the American Society for Industrial Security, Fortune 1000 companies sustained losses of more than \$45 billion last year from thefts of proprietary information, and a survey by the Computer Security Institute indicates over half of 600 companies polled said they suspected their competitors were a likely source of cyberattack. "Your competitors no longer have to be across town, or even across the country; they're in other countries that have different laws and business ethics," says Richard Power, who conducts the annual CSI survey. "Culpability is much less. There is a lawless frontier in terms of theft of trade secrets." Experts agree that while juvenile hackers often leave calling cards enabling them to be traced, professional information thieves are almost impossible to catch. What's even more frustrating is that many firms never know their systems have been breached. "It's difficult for people to see the theft of information," says the owner of a security firm. "Information is the only asset that can be copied or stolen but nothing can appear to be missing. You can still have the information... but have lost the value of that information." (MSNBC 11 Sep 2000)





2000-10-04 **Keywords:** security software sales

NewsScan (reprinted with permission), E-Commerce Times < http://www.ecommercetimes.com/news/articles2000/001004-1.shtml >

#### Vol #

Sales of security software are taking off, fueled by an epidemic of hacker attacks and vicious viruses, according to a study by Gartner Group's Dataquest division. Spending will soar from \$2.5 billion in 1999 to more than \$6.7 billion in 2004, as management software vendors, such as Computer Associates, IBM/Tivoli and Hewlett-Packard, increasingly focus on security in their core software offerings. According to the report, the top security software seller is antivirus protection, with 31% of the current market. According to the FBI, 9 out of 10 companies have reported computer security breaches -- including hacking, viruses, fraud and sabotage -- since March 1999. That study was based on a survey of 600 companies and government agencies. (E-Commerce Times 4 Oct 2000)





2000-10-17 **Keywords:** e-commerce security violations vulnerabilities exploits losses damage

availability quality assurance QA frustration incompetence bad design

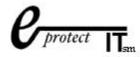
speed response time slow

NewsScan (reprinted with permission), E-Commerce Times < http://www.ecommercetimes.com/news/articles2000/001017-1.shtml >

Vol #

Technical and procedural glitches could cost e-tailers as much as \$15 billion in lost sales this holiday season, warns a new report by Creative Good. "The Holiday 2000 Online Shopping Report" concludes that nearly half of all would-be online shoppers will leave Web sites without making a purchase, and without contacting customer service. "If sites can simply make the buying experience easier, they stand to gain huge increases in revenue and a larger customer base who will return to shop after the holiday season is over," says a Creative Good analyst. "The sites that cannot convert shoppers to buyers this holiday season are likely to shut down in 2001." The survey, which looked at Gap.com, LandsEnd.com, Amazon.com, Barnesandnoble.com, BestBuy.com, Buy.com, eToys and KBKids.com, found that 43% of shoppers who visit a site intending to buy abandon their efforts due to frustration. Many of them then flee to bricks-and-mortar stores. The No. 1 reason for leaving the Web, cited by 40% of shoppers who changed their minds, was a cumbersome checkout process. Additional problems included slow-loading pages and inability to find the desired merchandise. (E-Commerce Times 17 Oct 2000)





2000-10-19 **Keywords:** infrastructure protection law enforcement criminal hackers cybercrime

attacks penetrations intrusions denial of service DoS meeting conference

international Internet OECD

NewsScan (reprinted with permission), Financial Times < http://news.ft.com/news/industries/infotechnology >

Vol #

The head of the National Infrastructure Protection Center, part of the FBI, warned that computer break-ins like the ones that plagued Yahoo!, Amazon and eBay last spring are likely to recur. Michael Vatis told policymakers and industry leaders meeting in London to discuss strategies for fighting cybercrime that it was "probable there would be another attack at least as successful" in the coming months. "All of the efficiencies and advances in productivity that have been created by the Internet have a downside. They make businesses more vulnerable." Organization for Economic Cooperation and Development officials warned that electronic breaches in the first two quarters of 2000 have outstripped all those for 1999, and said if the trend continues, it could undermine consumer trust in e-commerce. "The outlook is not encouraging," said Risaburo Nezu, head of OECD's directorate for science, technology and industry. "The response from consumers to new Internet business models is becoming cautious." The OECD is proposing it assume a larger role in tracking security breaches worldwide. (Financial Times 19 Oct 2000)





## **32.1 USA**

2000-01-26 **Keywords:** pornography filtering censorship university free speech law Edupage, Wired

Vol #

Republican Representative Jean McGrath (AZ) introduced new proposals for interfering with the viewing of pornography at state universities by restricting Internet access to "educational purposes" and by forcing universities to install censorware. Free-speech advocates and First-Amendment legal specialists protested that such legislation would be unconstitutional in the US.

2000-02-23 **Keywords:** filtering software censorship Internet library public filter shield

AP

Vol #

Voters in the Republican primary in Michigan on 2000-02-23 voted 4,379 to 3,626 against forcing the local public library to install censorware on their free public-access Internet terminals. The battle began when a child typed in "chocolate chip cookies" and the search returned pornographic pictures. Advocates of the filtering software were outraged that pornography was so easily accessible in a public institution; opponents said that filters are only 85% effective whereas the current strict policies of supervision ensure 99.9% compliance with the rules precluding visits to inappropriate sites. Library board members said they would rather shut down the library than install filters. Proponents of filtering worked closely with evangelical Christian organizations such as the Mississippi-based American Family Association, which contributed \$35,000 to the campaign.





2000-02-23 content filtering law library censorship **Keywords:** 

NewsScan (reprinted with permission), San Jose Mercury News

Vol

The city of Holland, a conservative 30,000-population town in the western part of Michigan, has defeated (with about a 55% margin) a proposal that would require the local public library to install filtering software on library computers so that children would be unable to access pornographic, violent, and hate sites on the Web. Apparently Holland is the first city to put this issue on the ballot, though it's been debated in many other places. One supporter of the defeated proposal said: "I just think that children really don't know what's for their own good. It may not be a really big problem at the library right now or in the future, but why take a chance?" An opponent of software filtering explained its defeat by saying: "I think free speech brought out a number of voters." (AP/San Jose Mercury News 23 Feb 2000)

2000-06-23 **Keywords:** children pornography free speech court case lawsuit judgement injunction **COPA** 

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/library/tech/00/06/biztech/articles/23privacy.html>

#### Vol

A federal appellate court . . . upheld a lower court injunction against enforcement of the 1998 Child Online Protection Act, a law intended to protect children from commercial Web sites trafficking in pornography. The three-judge panel ruled that the law, which required such sites to forbid access to Internet users who could not provide proof of their age, fell far short of meeting First Amendment standards of free speech. Though praising the efforts of Congress to protect children, the judges rejected the law's reliance on "community standards" to define pornography and asserted that it is impossible to simultaneously meet the moral standards of communities such as Chicago, Amsterdam, and Tehran. (New York Times 23 Jun 2000)





**Page 244** 

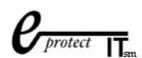
Category 32.1 USA

2000-08-09 **Keywords:** free speech censorship law judgement lawsuit ruling constitution NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/ap/docs/293190l.htm>

Vol #

U.S. District Judge J. Harry Michael Jr. . . . declared unconstitutional a Virginia law making it a crime to use the Internet to send children sexually explicit images or other materials that could harm them. The judge agreed with the civil liberties groups and Internet companies that had challenged the law as abridgment of the First Amendment right to free speech, on the grounds that there is no practical way to prevent children from accessing such material without also denying it to adults. (AP/San Jose Mercury News 9 Aug 2000)





2000-09-11 **Keywords:** survey study government infrastructure protection vulnerabilities weaknesses

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000911/t000085464.html>

#### Vol #

A . . . study released [in September] by the General Accounting Office has exposed widespread deficiencies in computer security in government agencies ranging from the Department of Interior to the U.S. Treasury. The report comes nine months after the President Clinton called on federal agencies to beef up security in his "National Plan for Information System Protection." That plan proposed that Congress boost federal spending for computer security and research by \$280 million to \$2.3 billion in 2001, but agencies say they need the money now. Government computer managers point to the tight labor market for computer security experts and say it's difficult to retain good personnel. The GAO report found that some agencies have failed to take even the most rudimentary steps to increase security, such as encrypting password files and limiting physical access to sensitive computers. In addition, agencies have been less than diligent about blocking access for independent contractors and former employees after they've left the government. In one agency, 7,500 of 30,000 users were not deleted after 160 days of inactivity. "The federal government, outside the defense area, is worse than the private industry because good computer security is about regular maintenance and housekeeping -- and that's not one of the government's strong points," says Stewart Baker, a Washington, D.C. technology lawyer. (Los Angeles Times 11 Sep 2000)





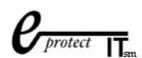
2000-10-30 **Keywords:** censorship filtering censorware pornography violence lawmakers legislation school children

NewsScan (reprinted with permission), New York Times < http://www.nytimes.com/2000/10/20/technology/20NET.html >

#### Vol #

Although a commission appointed by Congress has decided that parental involvement rather than software filtering is the right way to shield children from pornography on the Internet, senators John McCain and Rick Santorum and congressman Ernest Istook are introducing legislation to require schools and libraries to install software to protect children from encountering pornography and violence as they use the Web. Presidential candidates Al Gore and George W. Bush are both in favor of such filters. (New York Times 20 Oct 2000)





## 32.2 Non-USA

2000-01-25 **Keywords:** censorship hate speech Web international British UK England Edupage, Wired

Vol #

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.]

2000-06-07 **Keywords:** government censorship suppression freedom oppression dictatorship tyranny propaganda fear weakness human rights violations corruption news

NewsScan (reprinted with permission)

Vol #

Police in the Chinese city of Chengu . . . arrested 36-year-old Huang Qi on suspicion of "subverting state power" by operating the Web site www.6-4tianwang.com, which publishes information about human rights problems and corruption in China. If tried and convicted Huang could be imprisoned for more than ten years. (Reuters/San Jose Mercury News 7 Jun 2000)





2000-08-04 **Keywords:** censorship surveillance oppression dictatorship free speech monitoring Internet

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/internet/docs/278114l.htm>

#### Vol #

The Xinhua news agency in China is reporting that the Chinese government has created 20 or more special Internet police units around the country to "administrate and maintain order," investigate "criminal cases, such as cheating, property embezzlement, and pornography," and train volunteer "electronic security guards" for banks. Although the Chinese government routinely monitors the activities of its critics, the Xinhua report makes no mention of new government efforts to police political activities on the Internet. (Reuters/4 Aug 2000)

2000-10-03 **Keywords:** censorship government totalitarian fear restrictions policing content filtering ISP audit trail police law enforcement privacy encryption

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/200001003/t000093953.html >

#### Vol #

In its continuing effort to keep a lid on the impact of the Internet, China's government . . . issued new regulations that hold companies responsible for blocking illegal or subversive content, limit foreign investment, and threaten to close down any unlicensed operations. Internet content and service providers are directed to keep records of all content on their Web sites and all the users who dial into the servers for 60 days, and turn those records over to police on demand. "This creates a system that would require such a scale of enforcement that it could potentially occupy the whole efforts of ICPs," . . .[said] a Beijing-based Internet consultant. "Technology will respond. It will give rise to a whole new generation of encryption techniques." (Reuters/Los Angeles Times 3 Oct 2000)



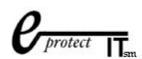


2000-11-07 **Keywords:** censorship privacy government restriction law chat e-mail news NewsScan (reprinted with permission), San Jose Mercury News < http://www.mercurycenter.com/svtech/news/breaking/merc/docs/023148.htm >

Vol #

The Chinese government has prohibited Web sites not owned by the state from offering news reports and has issued rules requiring that chat rooms engage only in officially approved topics. Portal sites will need special permission to offer news from foreign media. An executive of the portal site Sohu.com took an optimistic view of the new restrictions: "These were already the unwritten rules. In fact, this is better because we now know what the limits are." (AP/San Jose Mercury News 7 Nov 2000)





2000-11-29 **Keywords:** international law jurisdiction Web sites hate speech censorship

NewsScan (reprinted with permission), San Jose Mercury News

 $< htt://www.sjmercury.com/svtech/news/breaking/merc/docs/077786.htm> \ , \ Financial \ Times < http://news.ft.com/news/industries/infotechnology >$ 

#### Vol #

[In August,] France, where it is illegal to exhibit anything that incites racism, . . . [took] legal action against Yahoo! Inc. because its sites have been used for the sale of Nazi medallions, swastikas, etc. Yahoo has withdrawn customer postings of such items on its French site, fr.yahoo.com, but says it is not technically feasible to keep French users off of sites in other countries. In the U.S., extremist ideas are protected by the First Amendment of the Constitution, which guarantees the right of freedom of speech. (AP/San Jose Mercury News 11 Aug 2000)

[In November, a] Paris court . . . ordered Yahoo! to block French users from accessing Nazi memorabilia on its U.S. sites, citing French anti-racist laws. The ruling . . . [gave] Yahoo! three months to implement some type of system that would accomplish its objective and . . . [imposed] a FFr100,000 (US\$13,000) per day fine if it . . . [failed] to comply. Yahoo! had agreed to block the sale of such items on its French language portal following an earlier ruling, but had argued that the ban could not be extended to the U.S. site, both on U.S. constitutional grounds and because it was technically infeasible. But three court-appointed international experts concluded that a system to check the nationality of users, combined with password checks, would identify 90% of French citizens seeking to buy Nazi memorabilia. Industry groups are "deeply concerned" over the implications of the ruling: "Despite the obnoxious nature of the [Nazi] material, this ruling sets a very bad precedent for the future development of services on the Internet," says the head of the e-business unit at the Confederation of British Industry. (Financial Times 21 Nov 2000)

Internet experts Vint Cerf and Ben Laurie . . . [criticized] the decision of a French court to order Yahoo's U.S. portal site to prevent its customers from seeing auctions of Nazi memorabilia. Cerf, who is often described as the "Father of the Internet," . . . [said] that "if every jurisdiction in the world insisted on some form of filtering for its particular geographic territory, the World Wide Web would stop functioning." (BBC News 29 Nov 2000)

< http://news.bbc.co.uk/hi/english/sci/tech/newsid\_1046000/1046548.stm >





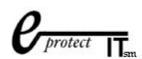
2000-12-04 **Keywords:** censorship monitoring anonymity identity repression totalitarian government regulation hypocrisy propaganda

NewsScan (reprinted with permission), San Jose Mercury News < http://www.mercurycenter.com/svtech/news/breaking/merc/docs/084179.htm >

Vol #

In announcing new rules to monitor activities on online bulletin boards, China's Minister of the Information Industry said: "Don't misinterpret this. The Chinese government absolutely is not saying people can't use these things, but we must find a more healthy way to manage them to ensure the protection of individuals' reputation and privacy. Anyone who has used the Web knows already that people always use false names. No one uses their own name. If someone attacks someone else there is no way to catch them, no way to sue them.'' (AP/San Jose Mercury News 4 Dec 2000)





# 33.1 Acceptable use

2000-02-19 **Keywords:** e-mail privacy policy openness awareness conflict monitoring ownership InformationWeek

Vol #

Thomas York summarized the state of e-mail privacy in an article for InformationWeek in February 2000. He cited a case that made news in November 1999 when the New York Times fired 23 workers in its Norfolk, VA support office for distributing offensive jokes through corporate e-mail. Despite the cries of protest from free-speech advocates, corporate America is increasingly making it clear to employees what has always been true: that corporate e-mail systems and the message that flow through them are company property. However, observers comment that it is unreasonable to bar all personal messages from the systems, especially when employers are glad to see staff working unpaid overtime. The essential rule is that employees must be aware that their communications are being monitored. In addition, employees can use outside e-mail systems (assuming they can get through company firewalls) for more privacy.





2000-03-10 **Keywords:** appropriate use management policy tools

NewsScan (reprinted with permission), MSNBC < http://www.msnbc.com/news/380471.asp>

Vol #

As employers increasingly worry about how to maintain control over workers' use of the corporate network for personal activities, such as e-shopping, or pornography perusal, a half-billion-dollar industry is taking off. Dubbed EIM, or employee Internet management, the new field comprises companies that make everything from Web filtering software to programs that track a worker's every keystroke. According to a new International Data Corp. white paper, Internet access control software was a \$63-million market last year, and is expected to evolve into a \$562-million EIM market by 2004. Currently, "660,000 companies are interested in buying these products," says IDC research director Chris Christiansen. Among those companies is Marriott International, whose senior technical analyst Scott Davis says, "Streaming medias are chewing up a lot more bandwidth than the HTTP protocol did in the past, and we have the HR departments and the corporate policy departments coming to us and telling us the (Internet) policy to implement." Policing those policies is increasingly difficult without adequate EIM software, he adds. (ZDNN/MSNBC 10 Mar 2000)





2000-04-25 **Keywords:** e-mail expectation of privacy monitoring intrusion employers employees labor relations government board regulations laws

NewsScan (reprinted with permission)

Vol #

Many companies now monitor their employee's e-mail and Web activities, assuming they have the inalienable right to ban personal or inappropriate use of office PC. But rebellious workers are now fighting back, using the National Labor Relations Act, a Depression-era law that sired the National Labor Relations Board (NLRB). The quasijudicial NLRB, which protects workers' rights to organize and communicate freely with each other about work terms and conditions, has weighed in on the employee's side in several recent cases involving workplace electronic monitoring activities. In one case, an employee fired for not apologizing over an e-mail he wrote criticizing a new vacation policy was granted back pay and a chance to rejoin his old firm (he took the pay but refused the job). In another, Pratt & Whitney was forced to back off a total ban on using the office e-mail system for non-business purposes. "The way people work is changing dramatically," says NLRB associate general counsel Barry Kearney. To keep up with the times, the NLRB is now asking branch offices to forward to Washington headquarters any cases involving e-mail or Web use by employees. (Wall Street Journal 25 Apr 2000)





2000-06-20 **Keywords:** intellectual property peer-to-peer access censorship surveillance filtering monitoring

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/044058.htm>

#### Vol #

Universities are struggling over the issues posed by Napster software, which allows people to make unauthorized copies of music. At a University of Southern California forum yesterday, attorney Cara Burns took a dim view of the idea of letting students use university facilities to steal copyrighted material: "There are certain cases when the university has to act as Big Brother. Is that what you send your kids to university for -- to download music? ... I am for new technology, but I'm also for artists and artists' right. Napster to me has more to do with stealing. Artists have the right to control their music." Taking a difference approach, USC chief information officer Jerry Campbell argued: "There is a serious principle involved here. We do not censor access... Trying to solve the problem in the courts is just stalling for time. Technology will not be rolled back by any law.'' (AP/San Jose Mercury News 20 Jun 2000)

2000-07-11 **Keywords:** privacy executive corporate title officer position responsibilities policy NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/032861.htm>

#### Vol #

A new executive position is showing up on the organization charts of companies such as American Express, Citigroup, Prudential, and AT&T: the Chief Privacy Officer, who has broad powers to protect the privacy of consumers who interact with corporate computer systems. George Washington University professor Lance Hoffman says that the new position "attracts people who have a knowledge of history and law. They know something about technology, and they can't get techno-dazzled by explanations that don't hold water. They appreciate what technology can do for good and for evil." (AP/San Jose Mercury News 11 Jul 2000)





2000-09-19 **Keywords:** appropriate use contract regulations agreements online auctions taste obscenity restrictions

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cti549.htm>

#### Vol #

Online auctioneer eBay has stopped the sale of an autopsy picture and crime scene photographs of three slain boys. A company executive said, "This was the first time a crime scene photo of a minor had been placed on eBay. It was also the first time, that we are aware of, of a coroner's photo being placed on the site. " He added: "We are dealing with some very tough issues because a lot of this type of merchandise is readily available in other arenas. We are also looking at a lot of legal issues involving the rights of people to sell things." But an attorney for the organization Parents of Murdered Children said: "We're not talking First Amendment, we're talking good taste," he said. (AP/USA Today 19 Sep 2000)





2000-10-01 **Keywords:** intellectual property IP copyright violations infringement music academia

universities colleges peer-to-peer appropriate-use policy bandwidth

saturation availability academia universities colleges policy

NewsScan (reprinted with permission), Los Angeles Times

< http://www.latimes.com/business/20000831/t000081672.html> , San Jose Mercury News

< http://www.sjmercury.com/svtech/news/breaking/ap/docs/465588l.htm>

#### Vol

A report by the Gartner Group . . . [said] 17 out of 50 -- about a third -- U.S. colleges and universities surveyed have banned students from using Napster on their campuses. Gartner says the song-swapping service is raising a number of moral and legal issues for school administrators, who are hurrying to establish policies regarding digital music sharing before campuses open for the fall session. Among colleges still allowing Napster use are Columbia, Harvard and Stanford, while New York and Kent State universities have instituted bans. (Los Angeles Times 31 Aug 2000)

Colleges and universities are split on "the Napster issue." Some are blocking Napster, some are not. Among the ones that are not are Georgia Tech, Michigan, Stanford, Duke, and the University of California at Berkeley. A Georgia Tech official says: "We are an educational institution and we will err on the side of unfettered access to information. Once you start down that road ... well, we could tie up an awful lot of staff people and resources trying to evaluate Web sites' content, and we don't want to get into that." Among the ones that are blocking Napster are Yale, Indiana, Southern California, Texas, Ohio State, Northeastern, and Canisius. The first three in this group made their decisions after being sued by two rock groups and the Recording Industry Association of America; the second two chose to block Napster on the grounds that Napster traffic clogged their computer networks; and the last two cited legal and ethical reasons for rejecting Napster and similar programs. A Canisius official explained: "It's not free for you to steal books from the public library, and it's not free to download music you haven't paid for." (AP/San Jose Mercury News 1 Oct 2000)





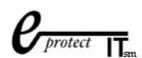
2000-11-12 **Keywords:** appropriate use monitoring covert channel chat

NewsScan (reprinted with permission), Excite < http://news.excite.com/news/ap/001112/00/cianaughty-chat >

Vol #

Although their "misuse of computers" did not compromise any classified information, 160 employees of the Central Intelligence Agency are being investigated for exchanging off-color messages on a private chat room that had been set up covertly on the Agency's classified internal network. One CIA official said that if those agents who created the covert communications facility had put it on the KGB's system "we'd be giving them medals," but that "sadly, it was ours." (AP/ExciteNews 12 Nov 2000)





2000-12-20 **Keywords:** covert channel confidentiality unaware social engineering detailed information auto-reply abuse danger vulnerability

**RISKS** 

**Vol** 21 # 16

Dan Birchall wrote an excellent piece for RISKS about the dangers of inadvertently revealing too much information by creating an overly-explicit auto-response for email when one is away from the office. As he pointed out, a detailed message may be OK for close colleagues but wholly inappropriate for publication; for example, "I will be away from [government laboratory] from [departure date] and will return on [return date]. If you need to reach someone from the IT Security staff, Please contact [coworker] at [number] or e-mail to [address]." Such a message is far too revealing for strangers, some of whom may be interested in competitive intelligence (e.g., which conferences you are going to) and others who may be hackers or industrial spies interested in social engineering. Subscribers to e-mail distribution lists may not realize that their autoresponder messages are going to total strangers. Birchall concluded, "send something like this:

> I am currently away from work. If you need to reach someone, please contact John < jsmith> at 555-1212.<

The logic, of course, is that an authorized person already knows where you work, what you do, your e-mail domain, and your area code. Nobody needs to know how long you'll be gone, if there's someone else who can help them."





# **33.2 Spam**

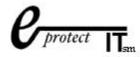
2000-01-19 **Keywords:** pornography unsolicited commercial e-mail junk spam pornography fraud deception hyperlink source

**RISKS** 

**Vol** 20 # 77

Pornography-promoters have taken to inserting innocuous labels for URLs such as links to electronic postcards but actually linking to hard-core sites. One RISKS correspondent noted that linking to such sites at work can cause difficulties for employees. MORAL: do not link to URLs from people you don't know without checking the actual destination.





2000-02-16 **Keywords:** mailstorm junk unsolicited commercial e-mail closed list RISKS

**Vol** 20 # 79

Junk e-mailers were reportedly using closed e-mail lists as a form of spam relay for unauthorized mail. Using a forged header including the desired target's e-mail address as the REPLY-TO or FROM address, the criminal sends the junk e-mail to a closed list which bounces the entire message to the victim along with notification that the victim is not authorized to post to the list. Recommendations [from MK]:

- A) Turn off automated notification of rejection altogether on all closed lists; or if you feel that the notification messages are important, then
- B) Configure the listserv to send back only the title of a rejected message, not the complete text; or if you feel like addressing the potential vulnerability head-on,
- C) Design a check of a log file so that the listserv for a closed list can quickly identify a mailstorm and stop it by turning off automated notification of rejection when it is being abused.





2000-04-11 **Keywords:** spam unsolicited commercial text junk advertising unscrupulous creeps jerks idiots sociopaths

NewsScan (reprinted with permission)

Vol #

Spammers have started using the text-messaging services on some cell phones to send unsolicited messages, probably by simply trying consecutive numbers until they find valid ones. An executive of a company called Plugout.com, which sends unsolicited text messages about its products, says: "What better way to reach your target market? [The company sells cell phone accessories.] We look at it as if we're doing these people a favor if they're looking for these kinds of products." One irate AT&T Wireless customer replied: "Clearly the sender knows it's going to interrupt somebody's day... They're not doing me any favors by soliciting me over my cell phone." (Washington Post 11 Apr 2000)

2000-07-12 **Keywords:** spam e-mail relay design

**RISKS** 

**Vol** 20 # 95

Google allows anyone to "e-mail these results to friends" for its search results. However, as Lloyd Wood pointed out in RISKS, one can erase the generated text and put anything one wants in the message, providing an anonymizing relay for unsolicited bulk e-mail.





# 33.3 Antispam

2000-01-11 **Keywords:** spam unsolicited commercial e-mail opt out Web service marketing Edupage, New York Times

Vol #

Anti-spam activists howled with derision as the Direct Marketing Association launched e-MPS, a Web site that requires consumers to opt out of receiving junk e-mail from those few spammers who care about consumer preferences.

2000-01-24 **Keywords:** spam unsolicited commercial bulk e-mail advertising NewsScan, Los Angeles Times < http://www.latimes.com/business/20000124/t000007408.html >

Vol #

A study by Ernst & Young had depressing news for anti-spam activists. About 14% of US consumers who receive junk e-mail actually click on the URLs in the messages (although it wasn't clear whether they were trying to complain or actually interested in the products). Apparently this rate of click-through was 3 to 10 times higher than for banner ads. Brace yourselves for continued onslaughts of garbage from unscrupulous low-lifes sending out millions of unwanted messages so as to trap a few victims in their web of greed. [Aw, come on -- tell us how you really feel, Mich.]





2000-03-24 **Keywords:** spam unsolicited commercial e-mail law court judgement ruling decision first amendment

NewsScan (reprinted with permission)

Vol #

For the fourth time in three years, a federal or state judge has ruled against a state-level attempt to legislate Internet spamming, on the grounds that is in violation of the Constitution's commerce clause, which specifies that a state cannot pass a law concerning activity within its borders if the law's local benefits are outweighed by the burden it imposes on the interstate flow of goods, services, or information. The most recent decision comes from a Washington state Superior Court in Seattle. Professor Jack Goldsmith of the University of Chicago Law School predicts that the issue will ultimately be decided by the U.S. Supreme Court: "It's going to be fascinating," he predicted. "The current justices tend to be pro-states' rights, and they're going to be sympathetic to some of these state regulations. On the other hand, many people think state regulations of the Internet are a drag on the development of the Net, and the Court has shown a broad sympathy to that point of view, too." (New York Times 24 Mar 2000)





2000-05-19 **Keywords:** spam filter pornography QA quality assurance design flaws false positives rules criteria

**RISKS** 

**Vol** 20 # 89

Gary Cattarin analyzed the antispam filters in MS-Office 2000's Outlook program. The assumptions behind MS engineers' spam-identification rules resulted in false positives (non-spam being identified and filed as spam). For example, the rules included > Body contains ",000" AND Body contains "!!" AND Body contains "\$" < and therefore caught an inoffensive non-spam message from Cattarin to one of his friends. Analysis of the porn filters for Outlook 2000 revealed the following rules as described by the correspondent (material between > and < is a direct quotation): > Subject contains "sex"

Subject contains "free" AND Subject contains "sex"

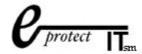
The first is set up with a leading space to only accept the \*word\* "sex", so those of us who live here in Middlesex county don't lose any local-related mail. But the writer of the second wasn't so careful -- what if the Middlesex News offers free subscriptions? That's Spam, yes, but not porn (I guess that's why that newspaper changed its name...).

(2) Don't address your dear friend as such -- note the rule:Body contains "Dear friend"My golly! I can't send some good old-fashioned heartfelt feelings to my dear friends!!

[Peter G. Neumann decided to print the entire analysis of the filtering rules in a separate issue (20.89x) for fear that the normal issue of the RISKS Digest would be blocked because of the key words and phrases in the report itself.]



(oops, double "!!" -- I got excited!)<



2000-06-05 **Keywords:** antispam signature strings filters false positive errors restrictive RISKS

**Vol** 20 # 91

William Coburn illustrated the risks of relying on generic strings when trying to identify unsolicited commercial e-mail ("spam"). Two of the strings he used to use were "friend@" and "@public.com" in the e-mail header FROM field. By monitoring the rejection log, he was able to discover that e-mail from a legitimate correspondent called Mr Friend had also been blocked. When he informed the hapless Friend, this chap commented that he had wondered why so many of his e-mail messages apparently went astray. Coburn concluded, "he risk here, is that automated processes can chug along for years without anyone ever noticing that they are broken."

2000-07-19 **Keywords:** spam unsolicited commercial e-mail junk criminals fraud forgery e-mail return address penalties

NewsScan (reprinted with permission)

Vol #

The U.S. House of Representatives passed 427-1 a bill that would require senders of unsolicited commercial e-mail messages to provide a valid return e-mail address that recipients of the messages could use to take them off the mailing list. Under the law, the Federal Trade Commission could bring legal actions again spammers who willfully ignore it. Violators could also be sued by Internet service providers. (AP/USA Today 19 Jul 2000)





2000-08-03 **Keywords:** spam unsolicited commercial e-mail junk lawsuit opt-in surveys

NewsScan (reprinted with permission), New York Times

< http://www.nytimes.com/library/tech/00/08/biztech/articles/03spam.html>

Vol #

Online market research Harris Interactive, which regularly conducts surveys of 1.5 million registered participants, is suing America Online and other Internet service providers it claims used the service of a nonprofit organization known as MAPS to illegally block e-mail from Harris survey participants. MAPS is an acronym for Mail Abuse Prevention System, and the service it provides is called the Realtime Blackhole List. The Harris lawsuit, which also names as defendants such companies as Microsoft Hotmail, BellSouth, Juno Online Services, and Qwest Communications, says that it never sends unsolicited mass mailings and that all of its survey participants have voluntarily registered to receive Harris questionnaires. (New York Times 3 Aug 2000)

2000-09-25 **Keywords:** unsolicited commercial e-mail junk industry consortium alliance association regulation complaints privacy standards

NewsScan (reprinted with permission), Wall Street Journal <

http://interactive.wsj.com/articles/SB96982808494289528.htm>

Vol #

Several leading e-mail marketers, including DoubleClick and 24/7 Media, . . . banded together to form the Responsible Electronic Communications Alliance, which plans new "privacy protection standards" aimed at reducing spam e-mail. The proposed standards are based on guidelines issued by the Federal Trade Commission, including giving recipients a way to register complaints and "opt out" of further mailings. The companies acknowledged that their move to establish standards is an effort to forestall government regulation: "The industry came together because it recognizes that if it's going to grow and prosper it's got to respect privacy, and we're not unaware that if we don't go ahead and do it, the government might," says Washington lawyer Chris Wolf, who will serve as the group's president. (Wall Street Journal 25 Sep 2000)





# 34 Net filters, monitoring (technologies)

2000-07-20 **Keywords:** workplace monitoring surveillance controls civil liberties employees employers covert law proposal legislation

NewsScan (reprinted with permission),

Vol #

A group of bipartisan lawmakers . . . introduced legislation that would require companies to disclose their workplace monitoring activities to employees when they are hired, and to update them on an annual basis. Under the bill, employers could still secretly monitor an employee if there is "reasonable" suspicion that illegal activity is taking place, but workers could not be routinely monitored without their knowledge. The American Management Association reports that 45% of companies with 1,000 or more employees snoop on workers in some way, but Sen. Charles Schumer (D-NY), a co-sponsor of the bill, says the figure is closer to 75%. "We would never stand for it if an employer steamed open an employee's mail, read it and put it back," says Schumer. "It is the same thing with an employee's e-mail." The bill has attracted a wide range of supporters, from the left-leaning American Civil Liberties Union to the conservative Eagle Forum. (MSNBC 20 Jul 2000)





# 34.1 Net filters

2000-01-29 **Keywords:** censorware filtering error

**RISKS** 

Vol 20 # 77

Some censorware (Internet filtering software) in libraries blocked access to the Superbowl XXXIV Web site because of the "XXX" string.

2000-03-16 **Keywords:** pornography libraries access children censorship filtering monitoring audit trail debate argument study research

NewsBytes

Vol #

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 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 Association (ALA) 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 for 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."





2000-09-22 **Keywords:** censorware pornography filtering photographs images algorithm InformationWeek

Vol #

Content Technologies announced a new pornography filter called Pornsweeper. the product looks at every incoming e-mail and attachment and differentiates likely candidates for rejection by the presence of too much "skin tone" compared with other colors in the image. Users determine the cutoff point.

2000-12-08 **Keywords:** censorware false positive incompetence stupidity RISKS, < http://sethf.com/anticensorware/smartfilter/gotalist.php>

**Vol** 21 # 14

In another spectacular demonstration of the importance of reverse engineering to expose incompetence, someone cracked the blacklist used by the SmartFilter censorware and discovered that several serious information security resources were erroneously blocked because they are classified in the "criminal skills" group: comp.risks, comp.dcom.telecom, comp.org.cpsr.announce, comp.org.eff.news, comp.protocols.tcp-ip, comp.security.announce and several others.





# 34.2 Usage monitoring, audit trails

2000-01-21 **Keywords:** privacy monitoring employer employee alert awareness expectation NewsScan (reprinted with permission), TechWeb < http://www.techweb.com/wire/story/TWB20000121S0014 >

#### Vol #

The newest version of Investigator, the software made by WinWhatWhere that's used by some companies to monitor employees' every keystroke, will add an optional banner alerting users to the presence of the system and telling them they are consenting to its use by operating the computer. Previous versions had been difficult to detect, leading some privacy advocates to complain about its sneaky intrusiveness. "I heard a lot of concerns about the invisibility of the program," says WinWhatWhere president Richard Eaton. "It had a splash screen that was just momentary, but this requires the user to acknowledge the message by clicking on a button before it goes away." (TechWeb 21 Jan 2000)

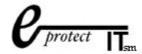
2000-02-11 **Keywords:** civil lawsuit seizure evidence disk drives subpoena investigation employees home computers protests labor action

POLITECH, World Socialist Web Site < http://www.wsws.org/articles/2000/feb2000/nwa-f11.shtml >

#### Vol #

In February, Northwest Airlines succeeded in getting a subpoena allowing their investigators to seize computers from the homes of 21 named employees whom the company accused of organizing and staging a "sick-out" that forced cancellation of many flights. Investigators copied data from hard drives, including private e-mail, and also searched computers at the offices of Teamsters Union Local 2000 in Bloomington, MN. Many advocates of free speech protested the action.





2000-04-18 **Keywords:** Internet filtering monitoring hardware

NewsScan (reprinted with permission), CNet < http://news.cnet.com/news/0-1004-200-1713007.html>

#### Vol #

Juniper Networks is shipping a new processor called Internet Processor II, a souped-up version of an earlier filtering technology that scans data flowing through a network to detect suspicious traffic. The Internet Processor II is capable of filtering 20 million packets of data a second, compared with older security software that could handle only 200,000 data packets per second. The older software slowed networks down so much that ISPs were reluctant to implement it. (News.com 18 Apr 2000)

2000-11-10 **Keywords:** privacy censorship monitoring lawsuit judgement decision education school records parents children teachers faculty staff

NewsScan (reprinted with permission)

#### Vol #

A New Hampshire judge has ruled that, since computers in schools are not for personal use but "as an integral part of the education curriculum," Internet history logs showing what sites are visited by students, faculty, and staff are public information open to inspection by any parent or parents willing to pay the cost of copying the information to disk after editing it to eliminate names and passwords of individual users. (New York Times 10 Nov 2000) http://partners.nytimes.com/2000/11/10/technology/10CYBERLAW.html





# 35.1 Cybersquatting

2000-01-21 **Keywords:** cybersquatting DNS trademark infringement

NewsScan (reprinted with permission), San Jose Mercury News http://www.sjmercury.com/svtech/news/breaking/ap/docs/115878l.htm

Vol #

Filing suit under a federal anti-"cybersquatting" law passed last year, musician John Tesh, who has a Web site called tesh.com to offer "intelligence for the family," is suing the owners of johntesh.com, charging that their only purpose in registering the site was to trade on his own good name and resell their domain name for a profit. (AP/San Jose Mercury News 21 Jan 2000)

2000-02-22 **Keywords:** trademark DNS domain name system conflict cybersquatting dispute arbitration

NewsScan (reprinted with permission)

Vol #

[By mid-February,] Eighty-nine cases [had] been filed with the "cybersquatting" arbitration service run by the World Intellectual Property Organization (WIPO) since its inception in December, and the service has already handed down decisions in favor of the World Wrestling Federation, Stella D'oro Biscuit, and Telstra. Still pending are disputes over dior.org, easyjet.net, world cup2002.com, jpmorgan.org, microsoft.org, alaskaairlines.org and dodialfayed.com. The mandatory dispute resolution system has seen a jump in cases from one filed in December to 60 filed in February. Unless an arbitrated decision is challenged in court, domain name registrars are bound to implement it. (Financial Times 22 Feb 2000)





2000-06-01 **Keywords:** domain name system DNS cybersquatting arbitration WIPO

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB959810376180166493.htm>

#### Vol #

Actress Julia Roberts . . . won control of the Internet name www.juliaroberts.com, after an international arbitration panel ruled that an accused cybersquatter had no legitimate interest in that name and registered it in bad faith. The World Intellectual Property Organization, which is one of four designated arbitrators of Internet domain name disputes, cited evidence that the defendant, Russell Boyd, had registered names of several famous movie and sports celebrities, and had even tried to auction the Roberts address on eBay. In reaching its quick decision, the panel is demonstrating its willingness to extend protection to famous individuals, even if they haven't formally registered their names as trademarks. (Wall Street Journal 1 Jun 2000)

2000-11-28 **Keywords:** censorship Web DNS domain name system lawsuit cybersquatting forgery judgement filtering

NewsScan (reprinted with permission), Wired < http://www.wired.com/news/business/0,1367,40380,00.html >

#### Vol #

A federal district court in San Jose ruled the. . . [sex.com] domain name must be returned to its original owner, from whom it was transferred six years ago through a forged letter. The successful plaintiff said that the ruling "shows that eventually the little guy an win at a great cost [\$500,000]" and added: "I plan to do something not as sick-o as this guy [the defendant]." The judge ordered the defendant to put \$25 million in escrow pending a determination of how much the plaintiff had been deprived by the misappropriation of the valuable name. . . . (Wired.com 28 Nov 2000)





2000-12-13 **Keywords:** DNS domain name service trademark copyright conflict

NewsScan (reprinted with permission), San Jose Mercury News < http://www.mercurycenter.com/svtech/news/breaking/ap/docs/743090l.htm >

Vol #

The Author's Guild has asked the Internet Corporation for Assigned Names and Numbers (ICANN) to require a British company called Old Barn Studios Ltd. to surrender ownership of domain names it created by appropriating the names of well-known authors, such as R.L. Stine, John Berendt, Charles Frazier, and Thomas L. Friedman. The Guild says: "For authors, whose names and reputations are their most valued stock-in-trade, bringing this proceeding was absolutely necessary. We hope to establish the precedent that in cyberspace, as in traditional venues of trade, authors' names belong to them, not to the first outfit that registers a famous name as a domain name." (AP/San Jose Mercury News 13 Dec 2000)





# 35.2 Trademarks vs DNS

2000-01-07 **Keywords:** Web DNS squatting trademark infringement lawsuit

NewsScan (reprinted with permission), Reuters, San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/000077.htm>

### Vol #

Teen Magazine has filed a federal lawsuit charging the operators of pornographic Web site of violating "cybersquatting" laws when it created a pornographic Web site called teenmagazine.com. Teen Magazine's own Web site is called simply teenmag.com. Lynn Lehmkul, an executive of the company that owns the magazine, says, "This is just unconscionable. It would be irresponsible of us not to pursue this matter in every possible way. It has been pretty well documented that people who seek out pornographic sites on the Internet use 'teen' as a search word." (Reuters/San Jose Mercury News 7 Jan 2000)





2000-01-25 **Keywords:** DNS conflict lawsuit infringement art corporation judge trademark POLITECH < http://slashdot.org/yro/99/12/01/2156208.shtml>

Vol #

In 1994, a group of European artists chose the DNS entry "etoy.com"; their Website went online in Oct 1995 and they proceeded to have fun for the next several years carrying out disrespectful creative acts such as hijacking Playboy pages using fraudulent metatags to get novice Web users onto the etoy.com Web site. The group continued in this jolly way until September 1999, when a company called eToys.com sued the etoy.com group for trademark infringement — even though eToys.com wasn't formed until June 1997 and did not reach the Web until October 1997. On Monday 29 Nov a (computer-illiterate?) judge granted the eToys corporation an injunction that forced etoy.com to shut down its Web site until the end of December 1999. In the intervening months, the unscrupulous business people saw the value of their stock go down thanks to a world-wide campaign of harassment against the litigious corporation, ably led by the (R)TM)ark organization. On 2000-01-25, eToys.com finally dropped its lawsuit.

2000-07-13 **Keywords:** cybersquatter trademark lawsuit domain name system DNS NewsScan (reprinted with permission)

Vol #

The International Olympic Committee, the U.S. Olympic Committee and the Salt Lake Organizing Committee . . . joined together in a lawsuit accusing some 1,800 Web sites of misusing the Olympic name. The suit represents the largest action by far brought under the recently enacted Anticybersquatting Consumer Protection Act. Previously, the largest named about 250 defendants. The IOC says about 50 of the sites have been turned over to the Olympic groups without further legal action. (AP/MSNBC 13 Jul 2000)





2000-10-16 **Keywords:** DNS trademark conflict lawsuit ruling judgement celebrity pornography NewsScan (reprinted with permission)

#### Vol #

Madonna . . . joined such celebrities as Julia Roberts and Isabelle Adjani in successfully suing a Web entrepreneur who created a site called madonna.com. The World Intellectual Property Organization found that the businessman, who used the site for sexually explicit material, "lacks rights or legitimate interests in the domain name" and that the name "had been registered and used in bad faith." (AP/MSNBC 16 Oct 2000)

2000-12-11 **Keywords:** DNS domain name system obscenity freedom speech lawsuit judgement ruling

NewsScan (reprinted with permission), San Jose Mercury News < http://www.mercurycenter.com/svtech/news/breaking/merc/docs/026011.htm >

#### Vol #

A federal judge has ruled against plaintiffs who relied on First Amendment rights to incorporate obscene or vulgar words in the addresses of the "adult" Web sites. Arguing that Web names are not only to provide addresses but also to communicate the nature of the product, their attorney gave the example: "When you're looking for antiques, the first thing you would put in is antiques.com." (And when you're looking for ... ) American Civil Liberties Union attorney agreed that domain names are "more than just signposts," but the position of University of Miami law professor Michael Froomkin is that the judge's ruling prevents individuals from arguing that domain names are simply words in the public domain, that can be used by anyone. (AP/San Jose Mercury News 11 Dec 2000)





# 35.3 Politics of the DNS

2000-03-17 **Keywords:** DNS domain name system jurisdiction cybersquatting legal ruling NewsScan (reprinted with permission)

Vol #

A federal court in Virginia has ruled that it has jurisdiction over all of the .com, .edu, .net and .org Internet domain names held in the vast registry of Network Solutions, which until recently held a monopoly over domain name registrations. The decision arose earlier this month as the court presided over the case of Caesars World Inc. vs. Caesars-Palace.com. Domain name disputes can be settled without going to court, via the arbitration procedures set up by ICANN and the World Intellectual Property Organization, but if plaintiffs decide to litigate, this ruling means they must answer to the Virginia federal court. "If you lose, all you lose is the property in Virginia" i.e., the domain name, "and not \$10 million in damages for trademark infringement," says an expert on legal jurisdiction, although she notes that the names themselves can be very valuable. (Financial Times 17 Mar 2000





2000-06-14 **Keywords:** DNS domain name system registrar invoice bill RISKS

**Vol** 20 # 92

Peter G. Neumann summarized an embarrassing lapse of DNS registration: "J.P. Morgan & Company (worth \$21 billion) lost its Internet connectivity on 13 Jun 2000 because they failed to pay their \$35 bill from Network Solutions for their jpmorgan.com domain: three bills ignored over six weeks. All of their Net customers were affected. (Last year Microsoft failed to reregister a domain name necessary for Hotmail service, although a computer consultant bailed them out by paying the fee for them.) "

In a follow-up contribution to RISKS, Peter Sleggs reported that he has experienced difficulties with Network Solutions' billings. On occasion, he failed to receive paper invoices for one of the two domains he has registered. In addition, his payments for one of the domain failed to be registered correctly. [Comment by MK: at this point, DNS registration is becoming a critical issue for businesses; perhaps a few good tort lawyers could do some good to encourage DNS registrars to shape up and recognize the importance of their operations.]

Similarly, Arthur J. Byrnes reported in RISKS that Network Solutions Inc. claimed that they would send a snail-mail and e-mail warning 30 days before the renewal deadline; they did neither. He very sensibly wrote, "So, my personal experience makes me wonder where the blame actually lies in these stories. I know that if I worked for a dot.com, I'd be checking all of my employer's domains expiration dates."





2000-06-26 **Keywords:** domain name system DNS lawsuit

NewsScan (reprinted with permission)

Vol #

ICANN, the Internet nonprofit corporation chosen by the Clinton administration in 1998 to run the Internet's domain name system, . . . [was] sued by Afternic.com, a corporation in New York that claims ICANN has violated its own bylaws by refusing Afternic's application to become a registrar for Internet addresses, and by ignoring repeated requests for a meeting. ICANN, controversial from the start and now low on cash, has never denied an application for a company or group to be a domain name registrar, but has kept some (such as Afternic's) on hold. (New York Times 26 Jun 2000)

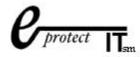
2000-07-10 **Keywords:** domain name system DNS government approval

NewsScan (reprinted with permission), New York Times < http://www.nytimes.com/library/tech/00/07/biztech/articles/10doma.html>

Vol #

The General Accounting Office (GAO), the investigative agency attached to Congress, . . . decided that the Clinton Administration acted within the law when it transferred to a nonprofit organization called the Internet Corporation for Assigned Names and Numbers (ICANN) authority to administer the registration of domain names for the Internet. Since its founding, ICANN has often been charged by critics who accuse it of being secretive and undemocratic. (New York Times 10 Jul 2000)





2000-07-17 **Keywords:** domain name system DNS trademark

NewsScan (reprinted with permission)

Vol #

ICANN, the global Internet name regulator, . . . approved a plan to expand beyond the seven top level Internet domain names, with the new addresses possibly appearing as early as . . . [2001]. The new names could include .shop, .bank, .travel, .museum and .sex, but no decisions on exactly which names would be added have been reached. Meanwhile, critics of the decision include groups that had lobbied for non-westernalphabet names and current owners of .com names who now must worry about protecting their trademarks by registering new names. (Financial Times 17 Jul 2000)





2000-07-23 **Keywords:** policy statement DNS domain name service politics RISKS, PFIR < http://www.pfir.org/statements/policies >

**Vol** 20 #

Lauren Weinstein and Peter G. Neumann, co-founders of the new group "People for Internet Responsibility" (PFIR, < http://www.pfir.org > ) published a manifesto entitled "Statement on Internet Policies, Regulations, and Control." The Executive Summary follows:

> It is increasingly clear that the Internet, as embodied by the World Wide Web and a wide variety of other Net-based services and technologies is rapidly becoming a critical underpinning and foundation to virtually every aspect of our lives, from the very fundamental to the exceedingly mundane. It is likely that few aspects of commerce, education, communications, government, entertainment, or any other facets of our daily existence will be unaffected by this exceedingly rapid change that is sweeping the globe far more rapidly than would have been anticipated only a few years ago.

These global and interconnected developments, unprecedented in human history, suggest that decisions regarding policies, regulation, control, and related Internet activities will be of crucial concern to the \*entire\* world's population. Consequently, the proper representation of many varied interests regarding such activities must be respected.

It is our belief that the current mechanism for making many key decisions in this regard, as embodied in The Internet Corporation for Assigned Names and Numbers, "ICANN" (http://www.icann.org), is proving to be inadequate to the task at hand. We believe that this is the result primarily of structural and historical factors, not the fault of the individuals directing ICANN's activities, whom we feel have been genuinely attempting to do the best possible job that they could with highly complex, contentious, and thankless tasks.

We are convinced that the Internet's future, and the future of humanity that will be depending upon it to ever increasing degrees, would be best served by consideration being given to the establishment of a new, not-for-profit, voluntary, international organization to coordinate issues of Internet policies and related matters. This organization would be based on a balanced representation of private-sector commercial and non-commercial interests, and public-sector interests including governmental bodies and organizations, educational institutions, and other





enterprises.

Although the proposed course of action is expected to be difficult, the risks of inaction are enormous and likely to increase dramatically in the coming years.

2000-10-20 **Keywords:** DNS conflict auction lawsuit

NewsScan (reprinted with permission), ZDNet< http://www.zdnet.com/intweek/stories/news/0,4164,2642661,00.html >

#### Vol #

A self-described "Internet entrepreneur" . . . filed a class-action lawsuit against Network Solutions Inc. [in October], charging the company with hoarding a stockpile of as many as three million domain names, which NSI plans to offer in a potentially lucrative auction. NSI tried to auction the names in May, but a public outcry forced the company to cancel its plans. If the suit is successful, NSI would have to make the expired domain names available to be registered through its public pool of names, rather than being sold off to the highest bidder. "They are attempting to benefit from a product that is not theirs," . . . [said] Scott Powell, the attorney for plaintiff Stan Smith. (ZDNN 19 Oct 2000)





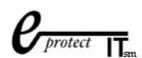
2000-11-03 **Keywords:** DNS domain name system registration lawsuit defamation fraud scam accusations

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cti760.htm >

Vol #

ICANN SUED FOR DEFAMATION The non-profit Internet Corporation for Assigned Names and Numbers (ICANN) is being sued in U.S. District Court in San Antonio by a start-up company called RegLand, which accuses ICANN of defamation and interference in its business. The company says that when it tried to pre-register new domain names, ICANN defamed it by calling it a "fraud" and a "scam." (Bloomberg/USA Today 2 Nov 2000)





 $2000\text{-}11\text{-}09 \qquad \textbf{Keywords:} \qquad \text{DNS domain name registration non-English characters conflicts IETF} \\ \text{NewsScan (reprinted with permission), San Jose Mercury News < \\ \text{http://www.mercurycenter.com/svtech/news/breaking/merc/docs/085037.htm} > \text{, InfoWorld} < \\ \text{NewsScan (reprinted with permission), San Jose Mercury News < } \\ \text{http://www.mercurycenter.com/svtech/news/breaking/merc/docs/085037.htm} > \text{, InfoWorld} < \\ \text{NewsScan (reprinted with permission), San Jose Mercury News < } \\ \text{http://www.mercurycenter.com/svtech/news/breaking/merc/docs/085037.htm} > \text{, InfoWorld} < \\ \text{NewsScan (reprinted with permission), San Jose Mercury News < } \\ \text{http://www.mercurycenter.com/svtech/news/breaking/merc/docs/085037.htm} > \text{, InfoWorld} < \\ \text{NewsScan (reprinted with permission), San Jose Mercury News < } \\ \text{http://www.mercurycenter.com/svtech/news/breaking/merc/docs/085037.htm} > \text{, InfoWorld} < \\ \text{NewsScan (reprinted with permission), San Jose Mercury News < } \\ \text{http://www.mercurycenter.com/svtech/news/breaking/merc/docs/085037.htm} > \text{, InfoWorld} < \\ \text{NewsScan (reprinted with permission), San Jose Mercury News < } \\ \text{http://www.mercurycenter.com/svtech/news/breaking/merc/docs/085037.htm} > \text{, InfoWorld} < \\ \text{NewsScan (reprinted with permission)}$ 

#### Vol #

In November, VeriSign, the company in charge of dot-com, dot-net, and dot-org Internet domain names . . . began accepting Chinese, Japanese, and Korean characters for those suffixes, an action expected to dramatically accelerate Internet globally. Arabic and other non-English languages will be added later. Doug Wolford, the general manager of Network Solutions Inc., VeriSign's registration arm, said: "There's a whole world out there that has really not been able to use the Web. Hundreds of millions of people have to use English to find their native language Web site. It's an absurdity, an artifact of history long outgrown." (AP/San Jose Mercury News 9 Nov 2000)

However, [t]he Internet Society . . . warned that proceeding with the sale of multilingual domain names will harm the stability of the Internet Domain Name System, and asked that the initiative be postponed until the Internet Engineering Task Force can develop a proposed standard for internationalized domain names. Internet Society VP David Maher admits that it's unusual for the group to issue such a strongly worded statement. "This is very significant... We think this will absolutely hurt the DNS and inevitably lead to conflicts as people claim to have the rights to certain names because of this test bed... Real problems come from the fact that there are conflicting proposals for how internationalized domain names should be handled. This automatically ensures there will be serious problems. It's like different companies selling telephone numbers or seats on the same flight." (Infoworld.com 8 Nov 2000)





2000-11-17 **Keywords:** DNS domain name system additions new opposition criticism costs

NewsScan (reprinted with permission), New York Times <

http://partners.nytimes.com/2000/11/17/technology/17DOMA.html > , San Jose Mercury News < http://www.mercurycenter.com/svtech/news/breaking/internet/docs/646427l.htm >

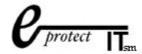
#### Vol #

[In November, the] Internet Corporation for Assigned Names and Numbers (ICANN) . . . [announced that it would] add seven new top-level domain names for Internet addresses:.info, .biz, .name, .museum, .aero, museum, and .coop. The first two will be for general use, with biz expected to relieve the pressure for businesses to find a unique name within the popular .com domain, which now has 20 million sites; .pro is intended for professionals, such as doctors and lawyers; .name will be used to designate personal Web sites; .museum will be restricted to museums; .aero for airline groups; and .coop for business cooperatives. ICANN did not give its approval to other domain names that had been proposed to it, including .web, .kids, .xxx, .union, .health, .travel, and .geo. The new names will not be put into effect no sooner than next Spring. (New York Times 17 Nov 2000)

The Geneva-based World Health Organization (WHO) . . . issued a statement expressing strong displeasure at ICANN's decision not to include a top-level domain name designated .health, and stating that the organization will "begin immediately to explore ways of recourse." WHO had proposed creation of a .health domain to be used strictly for sites providing information and services which met the quality standards of WHO and public health organizations, consumer groups, and academic institutions. (Reuters/San Jose Mercury News 17 Nov 2000)

[However, it] turns out that the seven new domain names chosen by ICANN may do little to broaden the possibilities for picking an Internet name. Many of the companies tapped to administer the new names are planning to restrict who can buy them by charging hefty registration fees and vetting those that apply. Neulevel, the company that will be administering the .biz domain, reportedly is planning to charge \$2,000 for each domain name and \$150 a year to renew it. It's also planning to make the .biz names available only to established companies in an effort to prevent cybersquatting squabbles. Many of the other organizations chosen to run the new domains are thinking about imposing similar restrictions. (BBC News Online 21 Nov 2000)





2000-11-30 **Keywords:** DNS domain name system conflicts politics

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB975524587449438763.htm >

#### Vol #

VeriSign's recent initiative to register Chinese-language Internet domain names has unleashed a maelstrom of conflict, with a Chinese government affiliate immediately launching its own rival, and incompatible, system. The result could be two separate Internet routing systems, causing major headaches for Chinese-speaking Internet surfers. "The risk is balkanization of the Internet, dividing the Internet up into islands of connectivity," says Pindar Wong, who until recently served as vice chairman of ICANN. "Global connectivity is the most precious aspect of the Internet. Anything that might potentially jeopardize that needs to be considered very carefully." The battle exemplifies Beijing's efforts to both embrace the Internet's development potential while at the same time attempting to control it. Critics say the system operated by the government-affiliated China Internet Network Information Center is as isolating as if China decided it would use its own system of telephone numbers. "It's a classic case of China trying to develop the Internet the way it suits them rather than what suits the rest of the world," says a senior analyst for IDC. (Wall Street Journal 30 Nov 2000)





# **Responses to intrusion**

2000-02-18 **Keywords:** intrusion honey pot monitoring logging audit criminal hacker penetration vandalism study report

San Diego Supercomputer Center < http://security.sdsc.edu/incidents/worm.2000.01.18.shtml >

Vol #

The San Diego Supercomputer Center set up an old workstation running Red Hat Linux as a honey pot to attract criminal hackers so they could be monitored. The "worm.sdsc.edu" machine was repeatedly penetrated and vandalized as security specialists watched and analyzed every step taken by the criminals down to logging every single packet used in the intrusions.





# **Education in security & ethics**

2000-05-22 **Keywords:** intellectual property copyright infringement theft counterfeit morality ethics open-source

NewsScan (reprinted with permission)

Vol #

Although some in the "open source" movement, which encourages the voluntary sharing of software source code, think that Napster and similar technologies are "influenced by the open-source ethic," Linux creator Linus Torvalds disagrees: "Piracy is bad. Of course you should be able to sue over copyrights." And Larry Wall, the developer of the Perl programming languages, agrees: "Open source should be about giving away things voluntarily. When you force someone to give you something, it's no longer giving, it's stealing. Persons of leisurely moral growth often confuse giving with taking." (Wall Street Journal 22 May 2000)





2000-09-22 **Keywords:** intellectual property IP music copyright violations infringement education training ethics awareness debate ambiguous complexity

children teenagers students over-simplification

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cti560.htm>

Vol #

In response to criticisms, the Justice Department has agreed to find "more precise" language for the following passage on its Web site answering the question "What is a cyber crime?" with the explanation: "Recently, tools have surfaced that allow Web users to download and save music from the Internet for free -- music that is copyrighted by artists and sold in stores. Taking tracks from the Internet is no different from stealing a CD or tape from a music store." Consumer Electronics Association president Gary Shapiro complains: "I'm offended the DOJ would fund a Web site which is telling millions of Americans they are committing a crime when they are not. This is wishful thinking by the (music industry). The fact is, my son is not a criminal; 20 million Napster users are not criminals." The position of American University professor Peter Jaszi, a Napster supporter, is: "There is a real question about what we should teach about copyright," Jaszi said. "Do we want to be telling people the whole story, which is a complicated story, which is all about rights and balances, or are we going to tell them a simplified story that they aren't going to believe or accept? If you try to simplify the message you are going to lose credibility." (USA Today 22 Sep 2000)





2000-10-10 **Keywords:** ethics education morality training schools law enforcement government parents educators

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/071435.htm >

#### Vol #

In alliance with the trade group Information Technology Association of America, the Justice Department has created a "Cybercitizen Partnership" program to encourage educators and parents to promote ethical behavior in cyberspace. FBI official Michael Vatis explains, "In a democracy in general, we can't have the police everywhere. One of the most important ways of reducing crime is trying to teach ethics and morality to our kids. That same principle needs to apply to the cyber world." (AP/San Jose Mercury News 10 Oct 2000)





# 41 New cryptanalysis techniques

2000-10-12 **Keywords:** decryption distributed computing international cryptanalysis

 $News Scan \ (reprinted \ with \ permission), \ New \ York \ Times < \\ http://partners.nytimes.com/2000/10/12/technology/12R-CODE2.htm > \\$ 

Vol #

A team of Swedish computer enthusiasts has succeeded in deciphering 10 increasingly difficult codes presented by author Simon Singh in his bestseller, "The Code Book." Singh, who has a doctorate in physics at Cambridge University in the U.K., took two years to develop the brain teasers with Dr. Paul Leyland, who works for Microsoft in Cambridge. The codes, which took the Swedes the equivalent of 70 years of computer time to decrypt, ranged from ciphers dating back to ancient Greece through the famed Nazi Enigma code machine used in World War II. The team was awarded a check for \$15,000 for their efforts. Team leader Fredrik Almgren said the task was extremely daunting and that he and his fellow scientists were tempted to abandon the effort several times: "The first stages were very simple but at one point we thought we wouldn't get any further than stage eight. When you do come to the 10th stage it is a question of heavy mathematics and rather difficult algorithms that I don't even claim to understand myself." (Reuters/New York Times 12 Oct 2000)





# 42 Crypto algorithm weakness, brute-force attacks, implementation flaws

2000-02-28 **Keywords:** encryption algorithm implementation broken cryptanalysis weakness

Crypto-gram

**Vol** 99 # 11

In late 1999, the DVD content-protection scheme called CSS (Content Scrambling System) was cracked and software to do so made available freely on the Internet. Cryptographer Bruce Schneier published a cogent summary of the situation in his Crypto-gram newsletter 99-11 < http://www.counterpane.com/crypto-gram-9911.html > . He explained that the problem lay in the fundamental model. Each DVD player has one of 400 different unlock keys. Every DVD has a decryption key that is required to read the data. The decryption key is encrypted 400 times — once with each of the unlock keys that could be present on any given DVD player. Unfortunately, this scheme fails because the computer must be able to put those keys into memory— and once in memory, a specially-crafted program can necessarily snaffle the decryption key. Schneier comments, "It might be a bitter pill for the entertainment industry to swallow, but software content protection does not work. It cannot work. You can distribute encrypted content, but in order for it to be read, viewed, or listened to, it must be turned into plaintext. If it must be turned into plaintext, the computer must have a copy of the key and the algorithm to turn it into plaintext. A clever enough hacker with good enough debugging tools will always be able to reverse-engineer the algorithm, get the key, or just capture the plaintext after decryption. And he can write a software program that allows others to do it automatically. This cannot be stopped." The only way protection can work in such a scheme is to put the algorithm into the hardware, he wrote — and it would have to extend to the monitor itself.





# 42.1 Weaknesses

2000-03-27 **Keywords:** encryption algorithm weakness decryption e-commerce

**RISKS** 

Vol 20 #

Stephen King's electronically-distributed book, \_Riding the Bullet\_, was released in encrypted form on the Web; decrypted formats quickly appeared. As Peter G. Neumann commented in RISKS, the incident provided " stark evidence of security weaknesses in PC-based eBook distribution systems" and "The episode has irked the companies developing such systems, who complain that export restrictions have kept them from using more powerful encryption techniques."

2000-03-31 **Keywords:** e-book electronic book cryptography crack

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB954465411569087773.htm/t000030180.html>

#### Vol #

Computer hackers cracked the software code that was designed to prevent multiple downloads of Stephen King's "Riding the Bullet" novella, confirming publishers' worries over the dangers inherent in electronic publishing. The e-book's publisher, Simon & Schuster, confirmed that at least two hackers downloaded the software necessary to read the book from Glassbook Inc., one of the Web companies given rights to distribute the book, and managed to break the encryption code that prevented more than one customer from having access to each electronic copy sold. Pirated copies of the book were then distributed to about six Web sites and chat groups. The publisher contacted many of the Internet service providers hosting the sites and had them shut down. "All the publishers are well aware there is no perfect technical solution to this problem," says Glassbook president Len Kawell. "We will do our best with technology; the rest is a matter of patrolling." (Wall Street Journal 31 Mar 2000)





2000-07-21 **Keywords:** cryptanalysis cracking DVD scrambling hackers free speech litigation lawsuit

Edupage, EE Times, NewsScan (reprinted with permission), New York Times, Los Angeles Times < http://www.latimes.com/business/20000818/t000077486.html>

#### Vol #

Over the course of 1999, several groups posted information about flaws in the Content Scrambling System (CSS) developed for DVD video players by the 4C group (IBM, Intel, Matsushita, Toshiba). The DeCSS software posted on the Net led to cancellation of the planned December 1999 launch of DVD-audio players (which use a related encoding scheme called CSS2) and postponed release of the new devices until mid-2000. Respected cryptographer Bruce Schneier pointed out that any decoding scheme suffers from a fatal weakness: the decoded data stream must be available somewhere to be able to display pictures or generate sound. Even the decryption keys, he argued, are available in cleartext in memory. "... [S]oftware content protection does not work. It cannot work," he said. Nonetheless, in January 2000, the Motion Picture Association of America (MPAA) sued the criminal-hacker support publication 2600.com and several Web site owners to get DeCSS program allegedly written by Norwegian teenager Jon Johansen off the Net. Free-speech advocates at the Electronic Frontier Foundation (EFF) argued that the copyprotection scheme should not be granted legal protection; 2600 called for street protests. The organization's Web site claimed that A missive on the 2600.com Website, meanwhile, claims that the issue was "whether you have the right to play DVDs on the computer of your choice and whether you should be able to see DVDs from other countries." The plaintiffs argued that the tool was promoting outright theft of their intellectual property.

[In July,] Eight movie studios . . . [went] to court charging that Eric Corley, who publishes the computer hacker magazine and Web site called "2600," has violated the law by distributing software that breaks the code used to encrypt DVDs. An attorney for the studios warned: "The threat of world copying is here and the process has begun. It will become an avalanche unless this court acts." A warning of a different kind came from the defendant's attorneys, who argued that a decision for the plaintiff would mean the end of "fair use," the concept that allows for limited and prescribed exceptions to general copyright rules. (New York Times 18 Jul 2000)

The Norwegian teenaged programmer Jon Johansen, who with two colleagues created the DeCSS software that breaks the encryption coding of DVD files, was called as a witness in the New York trial in which Hollywood studios are suing Long Island-based programmer Eric Corley for distributing the DeCSS software on the

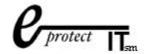




Internet, thereby encouraging illegal use of copyrighted movies. Corley's lawyer and the Electronic Frontier Foundation are defending his actions as an exercise of the Constitution's First Amendment right to freedom of speech. They argue that Corley never used DeCSS to pirate a movie, and that in fact to use the software to pirate movies would be impractical. (New York Times 21 Jul 2000)

[In August,] A federal judge ruled . . . against [the publisher of 2600, The Hacker Quarterly,] who posted software code that could be used to disable the electronic locks on DVDs, ordering defendant Eric Corley to remove the code from his 2600.com Web site as well as all links to other sites that post the DeCSS decryption code. The ruling came as a sweeping vindication of the entertainment industry's ongoing battle against piracy of copyrighted works. ". . . [The] landmark decision nailed down an indispensable constitutional and congressional truth: It's wrong to help others steal creative works," said Jack Valenti, chairman of the Motion Picture Association of America. The Electronic Frontier Foundation, which funded Corley's legal expenses, expressed surprise that the judge had also banned the links to other sites in his decision. "He is carving out a new exception for software under the 1st Amendment," said an EFF spokeswoman. (Los Angeles Times 18 Aug 2000)





2000-08-09 **Keywords:** intellectual property IP DVD encryption algorithm crack NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/articles/A58594-2000Aug8.html>

#### Vol #

Fearful that increasing numbers of pirated movies will be swapped on the Internet, Hollywood studios and the DVD industry have taken legal action against a Norwegian teenager who wrote code to break the encryption of DVD files. The suit also names as defendant the hacker magazine that posted the code on its Web site, as well as dozens of other Web sites that reposted it. Jack Valenti of the Motion Picture Association of America says: "We're putting a stake in the ground and saying you can't do this. You can't break this code, you can't put the code on the Internet, you can't have file-sharing with movies the way you do with music. We're going to protect our copyright." Duke University law professor James Boyle sees the MPAA position as a novel use of copyright law, since it targets the medium rather than the message: ""People think of copyright as prohibiting certain actions. You can't copy too much of something, you can't perform something without permission. What the content companies are starting to do is use copyright to regulate devices and research and communication. So now you can't communicate about a computer code." (Washington Post 9 Aug 2000)





## 42.2 Brute-force attacks

2000-01-17 **Keywords:** encryption algorithm cracked cryptanalysis brute-force parallel processing distributed

Wired < http://www.wired.com/news/print/0,1294,33695,00.html >

Vol #

The French systems integrator CS Communications & Systems developed a secret-key encryption algorithm and challenged cryptographers to crack a message encrypted with a 56-bit key. After 62 days of processing on 38,000 computers, the Distributed.net group cracked the message and won the \$10K prize. The parallel processing effort had to check 98% of the keyspace to find the key.

2000-02-17 **Keywords:** legal restrictions password decryption cracking tool burglary jurisprudence

Channel4000.com < http://www.channel4000.com/news/stories/news-20000217-164727.html >

Vol #

In Minneapolis, David Thomas Bell (33) was charged with 15 felony charges of unauthorized computer access, theft of trade secrets, attempted theft of trade secrets, computer theft, and possession of burglary tools. Nicole Lin Brelje (28) was charged with four felony counts. The defendants were accused of stealing a client list from Bell's former employer so they could take their business to Bell's and Brelje's new employer; the victim estimated the value of that list at \$2.5M. Investigation also suggested that Brelje had helped Bell run L0phtCrack, a password-guessing program, on their new employer's system. Bruce Schneier commented in his Crypto-Gram for 2000-03-15 < http://www.counterpane.com/crypto-gram-0003.html > that the interesting aspect of the case was the charge that using L0phtCrack constituted possession of burglary tools.





## **43.1 Tokens**

2000-10-10 **Keywords:** token smart card identification authentication I&A military government employee

NewsScan (reprinted with permission), New York Times < http://www.nytimes.com/reuters/technology/tech-smartcard-pentag.html >

Vol #

The Defense Department has taken the wraps off its new high-tech security badge, designed to control access to DoD buildings and computer networks. The new ID badge, dubbed a "common access card," features a magnetic strip and two bar codes, and will function as the standard ID for about 4 million people, including active duty military, selected reserve forces, civilian Pentagon employees and eligible contractors. The badge will also include a stored "certificate" that will enable the cardholder to sign digitally such things as e-mail and deployment orders. Although the badges are being hailed by DoD for their ability to enhance privacy through encryption, privacy advocates have voiced fears that the Pentagon could be laying the groundwork for the introduction of a national ID card in the U.S. "The military is frequently used as guinea pigs for proposals that would be too controversial to try among civilians," says David Banisar, senior fellow at the Electronic Privacy Information Center. "Ultimately, the danger is that people could be routinely tracked. Their records could be routinely used for purposes other than those originally intended." (Reuters/New York Times 10 Oct 2000)





## 43.2 Biometrics

2000-05-03 **Keywords:** biometric identification and authentication I&A fingerprint scanner personal computers

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000503/t000041568.html>

#### Vol #

Microsoft says it plans to incorporate biometric technology in its Windows software that will enable users to sign on by brushing their fingertips across a scanner rather than typing in a password. Biometric technology scans the details of a person's fingerprints, iris patterns, facial structure or other physical characteristics and compares them against a database of stored user information. The company will use authentication technology from I/O Software Inc. (Reuters/Los Angeles Times 3 May 2000)





2000-06-13 **Keywords:** intellectual property distribution encryption biometric I&A identification & authentication

NewsScan (reprinted with permission), New York Times < http://news.cnet.com/news/0-1005-200-2066437.html>

#### Vol #

Musicrypt.com and Net Nanny Software are teaming up to market an advanced "biometric" identification technology that would block would-be cyberpirates from distributing music free over the Net. In a new twist, the software identifies individual music listeners by the way they tap out letters on computer keyboards. This information is then used to protect songs against unauthorized distribution and use. The companies are hoping that music labels or online retailers will insert the technology into downloaded music, so that only a person who buys a given song would be able to play it on a computer. Identifying the buyer by these keystroke patterns is far more secure than using passwords, which can be passed on to thousands of people, the companies say. "What we're doing with (this software) is making the user the key," says John Heaven, Musicrypt's chief executive. One biometrics industry analyst notes that the keystroke technology is less accurate than other technologies such as fingerprinting or retinal scans, but it makes up for that weakness in its relative ease of use: "I would say that biometrics in general are ready for the consumer level. I wouldn't have said that two years ago. It would have been a disaster then." (News.com 13 Jun 2000)





# 43.3 Passwords

2000-01-15 **Keywords:** weak cryptography design error password crack vulnerability

Crypto-Gram < http://www.counterpane.com/crypto-gram-0001.html > ; ZDNet < http://www.zdnet.com/zdnn/stories/news/0,4586,2409537,00.html >

**Vol** 00 # 01

2000-07-14 **Keywords:** I&A identification & authentication credit history privacy

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/054775.htm>

#### Vol #

To identify online customers of the Checkfree bill-paying service, Checkfree will ask them questions based on their credit histories - such as what bank financed their car loans and what their mortgage payments are - and check their answers against information provided by the Equifax credit-reporting company.. An Equifax executive says: "Our strategy is to provide safety, security and privacy for Internet commerce transactions... It makes the application process for Checkfree easier for the consumer." (AP/San Jose Mercury News 14 Jul 2000)





## 43.4 Kerberos

2000-03-15 **Keywords:** Kerberos identification authentication I&A standards proprietary interoperability

Cryto-Gram

Vol 2000 # 03-15

Microsoft integrated Kerberos into its authentication scheme for Windows 2000; however, the company altered the protocol by using the "data authorization" field in a non-standard way. Microsoft ignored the rules for making changes to an IETF protocol and rendered their version non-interoperable with standard implementations of Kerberos. Bruce Schneier wrote, "On the surface, this is just nasty business practices. If you're a company that has invested in a UNIX-based Kerberos authentication system and you want to support Windows 2000 desktops, your only real option is to buy a Windows 2000 Kerberos server and pay for the integration. I'm sure this is what Microsoft wants.

My worry is more about the security. Protocols are very fragile; we've learned that time and time again. You can't just make changes to a security protocol and assume the changed protocol will be secure. Microsoft has taken the Kerberos protocol -- a published protocol that has gone through over a decade of peer review -- and has made changes in it that affect security. Even worse, they have made those changes in secret and have not released the details to the world. Don't be fooled. The Kerberos in Windows 2000 is not Kerberos. It does not conform to the Kerberos standard. It is Kerberos-like, but we don't know how secure it is."





# 44 New encryption algorithms, products

 $2000\text{-}02\text{-}28 \qquad \textbf{Keywords:} \qquad \text{encryption e-mail commercial free source code export restrictions} \\ \text{Crypto-gram} < \text{http://www.counterpane.com/crypto-gram-9906.html}> \text{, CMPnet} \\$ 

**Vol** 99 # 06

Hushmail < http://www.hushmail.com > and ZipLip offered free encrypted e-mail to anyone. Hushmail published its source code, which was not developed in the US, thus evading all US crypto export regulations. [Note that contrary to some mistaken news reports, it has never been illegal to use encryption in the US or to send encrypted e-mail or anything else encrypted out of the US. The only restrictions were on the encryption algorithms themselves.]





# 44.1 Algorithms

2000-06-30 **Keywords:** encryption anonymity distributed systems free speech

NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/articles/A21689-2000Jun29.html>

#### Vol #

Researchers at AT&T Labs have created a system called Publius that will make it very difficult trace the authorship or to remove files placed on the Internet without the direct participation of those who created them. The technology is described at www.cs.nyu.edu/waldman/publius, and works by encrypting and dividing files into pieces and then distributing them over a number of servers throughout the Web. A file's creator would be able to decide who and when it could be reassembled or removed. Called "Publius," the technology has been named in honor of American Founding Fathers Alexander Hamilton, John Jay, and James Madison who used that pseudonym when they anonymously published their famous "Federalist Papers." (Washington Post 30 Jun 2000)





2000-10-03 **Keywords:** encryption algorithm standard open

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/2000/10/03/technology/03CODE.html>

Vol #

The U.S. Department of Commerce . . . picked a new encryption standard to replace DES, the algorithm used for decades to scramble and unscramble messages and data between computer users. A play on the names of the two Belgian computer scientists who developed it (Vincent Rijmen and Joan Daemen), Rijindael is described in http://www.nist.gov/aes, along with the discussion surrounding its selection. The scientists are making their algorithm freely available. "We both make enough to have a decent life. We can buy the things we want to buy," said Mr. Rijmen. Ms. Daeman, looking to the future, added: "This makes us known. The fact that people know you as an expert, you can gain money, if you play it in the right way... I hope, I hope." (New York Times 3 Oct 2000)





# 44.2 Products

2000-01-27 **Keywords:** encryption algorithm

NewsScan, ZDNet, NEC press release, Investor's Business Daily < http://www.investors.com/>

Vol #

NEC's new Cipherunicorn-A encryption product was announced at the Encryption and Information Security Symposium in Japan at the end of January 2000. The new approach uses stealth techniques such as generating a number of false keys and varying the encryption keylength from 128 bits to 192 to 256 during the course of the stream encryption process. NEC researchers claimed that the new product would be the most powerful encryption tool in the world today, making practical cryptanalysis extremely difficult.





# 45 E-commerce security, digital signature, products, digital cash, e-payments

2000-08-31 **Keywords:** privacy surveillance covert channel data leakage confidentiality monitoring

NewsScan (reprinted with permission)

Vol #

The Denver-based Privacy Foundation . . . [said] that documents created with software that uses a hotlink shortcut to include images stored on a remote computer could be rigged to "phone home" to another computer and report where and how often a document is read. The technique, known as a "Web bug," is used in Microsoft word processing and spreadsheet applications, but is also found in other companies' software that uses automatic links to Web pages. "Because a linked Web image must be fetched from a remote Web server, the server is in a position to track when a Word document is opened and possibly by whom," says Privacy Foundation chief technology officer Richard Smith, who adds that there is no evidence anyone has exploited the arrangement. Web bugs can be as small as a single pixel, making them nearly invisible, says Smith. "In most cases, the reader of a particular document will not know that the document is bugged, or that the Web bug is surreptitiously sending identifying information back through the Internet." Microsoft program manager Eric Schultze says, "These [concerns] are not in any way specific to Microsoft or any other vendor, they are Internet issues. This could happen on any Web-enabled application or on any vendor's operating system." (Reuters/San Jose Mercury News 31 Aug 2000)





# 45.1 Digital signatures

2000-06-13 **Keywords:** e-commerce digital signatures contracts confirmation e-mail legislation proposal amendments

NewsScan (reprinted with permission)

Vol #

Proposed legislation on electronic contracts . . . attracted the attention of tinkerers in Congress, who . . . inserted a number of changes in the past few weeks, with one addition requiring Internet users to send a number of repeated e-mails reconfirming their consent to the contract at every stage of a transaction, as well as demonstrating that they had absorbed every bit of legal boilerplate. That change drew protests from the financial community, which viewed it as overly cumbersome, but the extra consumer measures also gave pause to Phil Gramm, chairman of the Senate banking committee. Gramm is less worried by brokerages than by the tendency among his fellow lawmakers to apply the old regulatory culture to the new online frontier, pointing out that the new bill goes beyond anything that already applies in contract law. "What happened to 'Let the buyer beware?'" he asks. "Common law and a thousand years of paper contracts established duties and responsibilities for people participating in commerce. You don't want to change that relationship so that ecommerce undermines contracts and commerce." The bill underwent further change yesterday to remove some of the obstacles, but as one financial expert said, "We have gone from having two different versions of a bill that would have been an A or an A minus, to a low B at best." (Financial Times 13 Jun 2000)





2000-06-15 **Keywords:** e-commerce digital signature law legislation

NewsScan (reprinted with permission)

Vol #

In a vote of 426 to four, the U.S. House of Representatives yesterday passed legislation that would make digital signatures legally binding. The bill had faced some opposition from consumer lobbyists, who worried that technology constraints might marginalize some consumers. The final language contains provisions for an "opt in" system where consumers must consent to receiving contracts and related information online. The bill does not specify any particular technology for creating digital signatures, leaving the issue open to competition in the marketplace. The Senate is expected to vote on the legislation in the coming weeks, paving the way for it to become law. (Financial Times 15 Jun 2000)

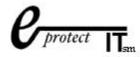
2000-06-25 **Keywords:** digital signature e-commerce alliances

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/080029.htm>

Vol #

Aided by new strategic alliances with Microsoft, IBM, Cisco, Sun and other technology partners, the iLumin Corporation plans to use its Digital Handshake technology to take advantage of recently passed federal legislation that allows "enforceable online transactions" using "signatures" that are actually heavily encoded scripts rather than images of handwritten signatures. The company says that digital signature technology will be used to facilitate \$135 billion worth of e-commerce transactions within two years. (Reuters/San Jose Mercury News 25 Jun 2000)





2000-07-05 **Keywords:** digital signatures e-commerce

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/ap/docs/167385l.htm>

#### Vol #

The co-founder of signOnline Inc., one of the tiny companies that hopes to take advantage of the new federal legislation on digital signatures, predicts: "Eventually, we're all going to have digital signatures. You're going to see the whole world transformed. This really does change the world." Who will profit from the expanded use of digital signatures? Besides companies such as signOnline, which sells digital signature technologies and services, the big winners will e-commerce security companies such as VeriSign Inc. and Entrust Technologies Inc., that provide universally recognized digital certificates. But there will be some losers as well, and shipment companies such as Federal Express and United Parcel Service will probably see lesser demand for their overnight document delivery services as the use of digital signatures becomes more common. (AP/San Jose Mercury News 5 Jul 2000)





# 45.2 Digital cash

2000-02-16 **Keywords:** e-commerce payment e-cash e-checks credit card currency NewsScan (reprinted with permission), Wall Street Journal

Vol #

A new system offered by PayPal.com allows registered users to use an e-mail message to send a cash payment to anyone with an e-mail account on the Internet. The sender writes an amount onto an online form, and that amount is charged to the sender's credit card or bank account. The receiver of the e-mail can then have the amount transferred to his or her bank or credit card account, mailed in the form of a printed check, or kept in the receiver's own PayPal account (which can be set up immediately) for recirculation. One happy customer says: "PayPal is replacing currency. This is becoming the payment service of the Internet." CheckFree and eBay are two other companies that will be offering similar services, and PayPal has signed up 190,000 customers since its launch [in late 1999]. (Wall Street Journal 16 Feb 2000)





# 45.4 E-payments

2000-02-17 **Keywords:** authentication certificates postage encryption online e-commerce

NewsScan (reprinted with permission), Wall Street Journal; Stamps.com

- < http://www.stamps.com/company/news/19991116a/> ; G2 TOR #193
- < http://www.g2news.com/BackIssuesTOR/TOR193.html#Stamps.com Loses Big>

#### Vol #

Event marketers like Ticktmaster.com, Tickets.com and Admission Network are moving quickly to implement technology that will enable customers to print their own tickets to rock concerts, sports events, and movies, but authentication of those do-it-yourself tickets is still an issue. Accordingly, they're turning to online postage sellers E-Stamp and Stamps.com to tap into their encryption technology and bar code techniques for secure online document printing. In response, Stamps.com, with backing from Paul Allen's Vulcan Ventures and some other investors, has formed EncrypTix Inc. to handle sales of event tickets, travel services and financial products like travelers checks. Forrester Research says of the three billion event tickets sold in the U.S. last year, about 10% were sold online -- a figure that's expected to grow significantly once the print-your-own model is ready for primetime. (Wall Street Journal 17 Feb 2000)

In a related article, G2 Computer Intelligence's "The Online Reporter" said, "Stamps.com posted an operating loss of \$41.8 million for the first quarter on revenues that rose 470% sequentially to \$2 million."





2000-03-01 **Keywords:** e-cash electronic payments e-commerce

NewsScan (reprinted with permission); < http://www.billpoint.com/>

Vol #

Billpoint, a new Internet payment method developed by eBay.com and Well Fargo, will allow individual buyers and sellers using eBay's auction services to complete their transactions using the buyer's credit card and the seller's bank account. Once the sale is completed, the purchase amount will be transferred immediately into the seller's checking account. (Wall Street Journal 1 Mar 2000)

2000-03-09 **Keywords:** e-cash e-money EFT electronic payments

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000309/t000022823.html>

#### Vol #

EMoneyMail, a unit of the Bank One Corp. in Chicago, has developed a service that, for a fee of \$1, will allow you to transfer to the account of another person (or a merchant) an amount up to \$500, which can be withdrawn from designated credit cards, debit cards, or checking accounts and sent via e-mail. The recipient of the transfer links to the EmoneyMail.com Web site, and can then direct the money into the preferred destination account. Jupiter Communications analyst Robert Sterling says, "We are seeing the beginning of a new, credible form of digital cash transfer. This could change the way people interact with their banks and how they use their credit cards." (Los Angeles Times 9 Mar 2000)





2000-04-05 **Keywords:** e-cash digital money electronic funds transfer payment NewsScan (reprinted with permission)

Vol #

The U.S. Postal Service is teaming up with CheckFree to allow customers to pay their bills electronically. The move pits the Postal Service directly against financial institutions like Bank of America and Citibank, which offer electronic bill-paying services, as well as Internet portals, such as Yahoo. Although banks will pose stiff competition to the new USPS service, because customers like to view their account balances before making payments, the postal service is likely to be favored over portals. "The advantage for the post office is the trust and comfort it brings to the table," says a securities analyst. "The post office may get a lot more customers than a Yahoo, which is viewed as fun and frolicky, but perhaps not a place to pay bills." IDC last month predicted that the electronic bill market will grow to \$1 billion by 2004. (News.com 5 Apr 2000\_)

2000-04-06 **Keywords:** e-commerce electronic funds transfer EFT payment

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/cutting/20000406/t000032183.html>

Vol #

The U.S. Postal Service, in conjunction with two corporations that offer electronic bill-paying services, has developed a new system called USPSeBillPay, which customers can use to pay all of their bills online. More detailed information can be found at http://www.usps.gov. (AP/Los Angeles Times 6 Apr 2000)





2000-09-12 **Keywords:** credit card fraud countermeasure one-time account numbers RISKS

**Vol** 21 # 05

Joshua M. Bieber reported in RISKS in September, "American Express will launch a disposable credit-card service in the US next month, designed to answer the worldwide worry of online shopping. The system, Private Payments, enables cardholders to access a random one-use only credit-card number with an expiry date on the AmEx website, to be used in making one online purchase. In the event that the number is illegally accessed during a transaction, it cannot be re-used by a hacker. Visa and MasterCard are also looking at similar ideas."

2000-09-22 **Keywords:** online bill payment digital money e-cash banks financial e-commerce NewsScan (reprinted with permission), E-Commerce Times < http://www.ecommercetimes.com/news/articles2000/000922-1.shtml>

#### Vol #

The number of households that pay their bills online will balloon from 100,000 currently to 40.2 million by 2005, according a report by Jupiter Research. The reports suggests that banks "forgo selfish interests" and form alliances with online electronic bill payment and presentation services in order to maintain a role in the process. "...Financial institutions must stop watching this market and start driving it. Fast-moving technology companies that want to control the billing and payment process are poised to take over the financial aspects of that customer relationship," says a Jupiter analyst. A report released earlier this year by IDC predicted that by 2004, electronic bill payment services will generate more than \$1 billion in revenue worldwide, compared with just \$32 million last year. (E-Commerce Times 22 Sep 2000)





2000-09-28 **Keywords:** online bill payment digital money e-cash banks financial e-commerce NewsScan (reprinted with permission), E-Commerce Times < http://www.ecommercetimes.com/news/articles2000/000928-1.shtml>

#### Vol #

Credit cards will soon begin losing ground to smart cards and other digital payment methods, as consumers grow more comfortable with e-commerce, according to a study by ActivMedia Research. The report predicts that credit cards, which currently account for 98.5% of online transactions, will decline to a 90% market share by next year, as new technologies move into the mainstream. At the same time, transaction volumes for smart cards and e-wallets will grow from \$500 million in 2000 to \$5.7 billion in 2001, and balloon to \$20 billion in 2002. "The ability to add an accentuated level of security is what people are striving for," says ActivMedia's VP for information services. Some credit card companies are already anticipating the shift witness Visa's new "smart Visa" rollout -- and analysts say "hybrid cards," which contain both an embedded chip and magnetic strip or bar code technology, are the next logical step. (E-Commercetimes.com 28 Sep 2000)

2000-10-12 **Keywords:** wireless e-commerce transactions security pact alliance consortium group cooperation

NewsScan (reprinted with permission), TechWeb < http://www.techweb.com/wire/story/reuters/REU20001012S0006 >

#### Vol #

Nokia, Motorola and Ericsson . . . [were] joined by Siemens in an alliance to develop secure mobile electronic transactions. The alliance, dubbed Mobile E-Business Technologies (MeT), will offer consumers a simple and safe way to conduct e-commerce transactions over their mobile phones. According to IDC, m-commerce, as it is called, will generate \$37.7 billion by 2004, up from \$51.2 million this year. (Reuters/TechWeb 12 Oct 2000)





# 45.5 Watermarks

2000-03-20 **Keywords:** digital watermark software tools e-commerce authentication Network World Fusion < http://www.nwfusion.com/newsletters/sec/0103sec1.html >

Vol #

Jim Reavis of SecurityPortal wrote a good overview of developments in digital watermarking for the Network World Security Newsletter in January 2000. He summarized the basic requirements for this image- and music-authentication technology: invisibility, accessibility, and resistance to modification. He also reviewed tools for creating and validating digital watermarks as well as developing services such as watermark-tracking, where a firm scans the Web looking for copyrighted works and reports on where they have been found.





2000-09-13 **Keywords:** criminal hackers contest vulnerability ethics watermark intellectual property IP music video movies encryption cracking vulnerabilities

#### Vol #

The Secure Digital Music Initiative, a forum of 175 companies in the music, electronics, information technology and telecommunications industries dedicated to developing a secure framework for the digital distribution of music, . . . [offered] a reward of up to \$10,000 to the first person to crack its codes. In an open letter to the "alternative" press, SDMI executive director Leonardo Chiariglione challenged hackers to "show off your skills, make some money, and help shape the future of the online digital music economy." SDMI has about 10 different proposals for "watermarking" technology that could be embedded in a digital music file. Portable music players complying with the SDMI standard would only work if the watermark -- an inaudible signal -- is present. SDMI has also issued the challenge to the technology departments at the University of California at San Diego, MIT, Virginia Tech and Stanford University. "The proposed technologies must pass several stringent tests: they must be inaudible, robust and run efficiently on various platforms, including PCs... So here's the invitation: Attack the proposed technologies. Crack them. By successfully breaking the SDMI protected content, you will play a role in determining what technology SDMI will adopt," said Chiariglione. (Financial Times 13 Sep 2000)

In November, [t]he Secure Digital Music Initiative (SDMI) . . . [said] that three out of five music-protection schemes tested withstood hacker attacks. . . . In announcing the results, SDMI executive director Leonardo Chiariglione refuted an earlier report by Salon.com that said all five technologies had been broken. "I'm an engineer, which means I deal with facts. We conducted all the tests that were planned and did not change the rules as we progressed. We came to the conclusion that not all the (technologies) had been hacked." The group is giving no details on which technologies prevailed, other than to say that both watermark and non-watermark proposals had passed the test. (CNet News.com 8 Nov 2000) http://news.cnet.com/news/0-1005-200-3583337.html





2000-10-24 **Keywords:** criminal hackers scientists contest vulnerability ethics watermark intellectual property IP music video movies encryption cracking

vulnerabilities

NewsScan (reprinted with permission), Associated Press/MSNBC < http://www.msnbc.com/news/480521.asp >

Vol #

A team of computer scientists at Princeton and Rice Universities and the Xerox Palo Alto Research Center (PARC) has been able to remove the invisible "watermarks" used by the 200-company Secure Digital Media Initiative (SDMI) to protect digital music files from pirates. SDMI had offered a prize to anyone who could defeat its various security measures, four out six of which make use of watermarks. SDMI's Tala Shamoon said, "I expected some would have fallen. This is part of an empirical process to get the best technology."

Professor Ed Felten and colleagues at Princeton University defeated all four of the schemes under test.

Vol #

Music subscription site EMusic.com has started using "acoustic fingerprint" technology, which it says can spot any of its 140,000 songs that are being illegally traded by Napster users. If such song-swapping is detected, EMusic will send an e-mail warning, asking that the swapping cease. Napster has apparently agreed to block the perpetrator's account if illegal trading persists, and if the user finds a way back into Napster through a different IP address, EMusic says it will try to block that person' Internet access. An analyst with Webnoize says, "This is a warning shot. They are saying they have the technical ability to track their music." He adds that the situation could lead to a lawsuit that would pit the two pioneers -- Napster and EMusic -- against each other. (ZDNet 21 Nov 2000)





# 45.6 Other e-commerce security measures

 ${\bf 2000\text{-}09\text{-}23} \qquad \textbf{Keywords:} \quad \text{artificial intelligence pattern recognition faulty design assumptions}$ 

reasoning credit card fraud prevention algorithm foolish

**RISKS** 

**Vol** 21 # 06

The CIBC (Canadian Imperial Bank of Commerce) has software that monitors buying patterns for its users. Unfortunately, a user and her husband discovered that their card had been frozen when they paid for a ferry to Vancouver, BC and the antifraud team received no answer at their home phone (because they were both on the ferry!). Rodger Whitlock commented in RISKS, "Badly thought-out computer wonkism strikes again."

A follow-up response from Perry Bowker suggested that actually, such pattern recognition really does stop fraud and that a solution to the problem described above is to carry two different credit cards, with one as a backup.





2000-12-01 **Keywords:** e-commerce litigation jurisdiction fraud complaint lawsuit regulation legislation

NewsScan (reprinted with permission), The Standard < http://www.thestandard.com/article/display/0,1151,20526,00.html >

Vol #

European justice ministers passed a law on Thursday that allows online shoppers to pursue disputes with e-commerce merchants in their own countries, rather than having to incur the expense and aggravation of dealing with a foreign legal system. The law, dubbed the Brussels I regulation, is essential to help get e-commerce off the ground in Europe, argued the justice ministers and the European Commission, which drafted the legislation. "A lack of consumer confidence is the main thing holding up the development of e-commerce here," said an EC spokesman. But industry representatives say this approach will create problems for smaller e-tailers: "For large companies it isn't a problem, because they have offices and lawyers in all EU countries. The SMEs (small and medium-sized enterprises) would be burdened with substantial legal and insurance costs if they took protection against litigation from outside their home market," says Wim Mijs, VP of EU affairs at Dutch bank ABN Amro. "As a result, venture capitalists might be a little more cautious about investing in a European Web venture." The EC regulation preempts less-stringent cross-border legislation currently under debate at the Hague Convention. (The Standard 1 Dec 2000)

 $2000\text{-}12\text{-}21 \qquad \textbf{Keywords:} \qquad \text{copy protection intellectual property hardware equipment politics protest} \\ \text{RISKS, TheRegister.com} < \\ \\ \text{http://www.theregister.co.uk/content/2/15620.html} > \\ \\ \\ \text{RISKS, TheRegister.com} < \\ \\ \text{http://www.theregister.co.uk/content/2/15620.html} > \\ \\ \text{RISKS, TheRegister.com} < \\ \\ \text{http://www.theregister.co.uk/content/2/15620.html} > \\ \\ \text{RISKS, TheRegister.com} < \\ \\ \text{http://www.theregister.co.uk/content/2/15620.html} > \\ \\ \text{RISKS, TheRegister.com} < \\ \\ \text{http://www.theregister.co.uk/content/2/15620.html} > \\ \\ \text{RISKS, TheRegister.com} < \\ \\ \text{http://www.theregister.co.uk/content/2/15620.html} > \\ \\ \text{RISKS, TheRegister.co.uk/content/2/15620.html} > \\ \\ \text{RISKS,$ 

**Vol** 21 # 17

John Gilmore published an anguished attack on the possibility that hardware vendors Intel and IBM were working on integrating copy protection into disk drives to preclude illegal copying of proprietary programs or data.





## 46 Cryptography exports from US

2000-01-13 **Keywords:** encryption export restrictions laws regulations

NewsScan, San Jose Mercury News

Vol

In January 2000, the Clinton administration finally gave up on the US government's futile attempts to restrict exports of strong encryption. Henceforth, only crypto sales to foreign governments or military would require US government authorization. What the State Department terms "rogue nations" would still be on the forbidden list (Iran, Iraq, Libya, Syria, Sudan, North Korea, and Cuba).

2000-01-15 **Keywords:** encryption export regulations

Crypto-Gram < http://www.counterpane.com/crypto-gram-0001.html >

**Vol** 00 # 01





 $2000\text{-}01\text{-}15 \qquad \textbf{Keywords:} \qquad \text{encryption relaxation restriction bill legislation proposal law} \\ Crypto\text{-}gram < \text{ http://www.counterpane.com/crypto-gram-0001.html} > ; PoliTech, Wired < \text{http://www.wired.com/news/print/0,1294,33672,00.html} >$ 

**Vol** 00 # 01

In January, the newly relaxed encryption export restrictions took effect. The main improvements were that all ordinary "retail" encryption products could be exportable once some paperwork was filled out — except to a list of forbidden terrorist countries. Any product with 65-bit keyspace could be exported without paperwork. Posting source code on the Internet was no longer restricted at all. Famed encryption expert John Young tested the new regulations by posting the binaries for PGP freeware v 6.5.2a for Windows and for Macintosh. The Department of Commerce published a response via Declan McCullagh's POLITECH list stating that in fact there was no problem with such posting.

 $2000\text{-}01\text{-}18 \qquad \textbf{Keywords:} \qquad \text{operating system Windows 2000 strong encryption export } \\ \text{Reuters , Wired} < \text{ http://www.wired.com/news/technology/0,1282,33745,00.html} > \\ \text{The export of the export o$ 

Vol #

Microsoft announced at the RSA Conference in San Jose, CA in mid-January 2000 that it had received US government authorization to sell its new operating system revision, Windows 2000, with 128-bit encryption enabled.





2000-02-02 **Keywords:** Export Administration Regulations EAR restrictions regulations government Commerce

NewsScan (reprinted with permission), MSNBC 1 Feb 2000 < http://www.msnbc.com/news/364870.asp>

#### Vol #

The Clinton administration has eliminated restrictions on exporting high-performance computers with speeds below 12,300 MTOPS (millions of theoretical operations per second) to all countries except so-called rogue nations (Iraq, Libya, North Korea, Cuba, Sudan and Syria). Companies exporting computers to "Tier III" nations (including China, Russia, India, Israel and Pakistan) would have to notify the Commerce Department 10 days prior to shipment of any computer operating above 12,500 MTOPS. Exports to "Tier II" countries (South Korea, much of Central and South America and most of Africa) will require licensing above 30,000 MTOPS (previously the threshold was 20,000 MTOPS). Clinton also called for Congress to shorten from six to four months the review period for adjusting export controls, noting the change is needed to "keep up with the rapid pace of technological advance."





2000-02-25 **Keywords:** encryption export restriction litigation

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB951422940442620073.htm>

#### Vol #

In an about-face, the U.S. government [said] it will allow computer scientist Daniel Bernstein to post the source code for Bernstein's Snuffle encryption software on his Web site. The change of heart came following a district court ruling that in light of the new, liberalized encryption software export restrictions implemented in January, Bernstein should be able to post his code. Bernstein and his lawyer are considering pursuing his lawsuit against the government, however, because "there's an area of ambiguity that remains": the new rules don't address "mirror sites," which copy and publish Web pages automatically to provide speedier access for users in other countries. The rules also require that the source code may be posted as long as residents of countries suspected of supporting terrorism won't have access to the material -- an administrative nightmare for any Web operator. (Wall Street Journal 25 Feb 2000)

2000-02-26 **Keywords:** encryption export regulations restrictions algorithm posting publication RISKS, Reuters < http://www.wired.com/news/politics/0,1283,34550,00.html > , Wall Street Journal < http://interactive.wsj.com/articles/SB951422940442620073.htm >

Vol 20 # 82

In February, the US Commerce Department gave up in its futile attempts to prevent Prof. Daniel Bernstein from posting details for his Snuffle encryption algorithm. According to Peter G. Neumann in RISKS, "the residual questions are on areas of ambiguity such as mirror sites and a restriction on access in countries suspected of supporting terrorism."





2000-04-05 **Keywords:** encryption export regulations restrictions lawsuit judgement EAR court NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB954899134353800815.htm>

#### Vol #

A federal appeals court in Ohio has ruled that encryption software code is protected by the First Amendment because such code is a means of communication between computer programmers. The ruling represents the first time that a federal appellate court has decided software code is protected as free speech, says Raymond Vasvari, legal director of the American Civil Liberties Union: "This is a great day for programmers, computer scientists, and all Americans who believe that privacy and intellectual freedom should be free from government control." The court's decision means a lawsuit filed by Cleveland law professor Peter Junger will be reconsidered. Junger had claimed that the government violated his free-speech rights by requiring export licenses for encryption programs. (Wall Street Journal 5 Apr 2000)

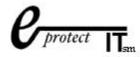
2000-07-18 **Keywords:** encryption policy controls regulations restrictions monitoring surveillance Internet traffic law enforcement investigation wiretaps interception

 $News Scan \ (reprinted \ with \ permission), \ Washington \ Post < http://www.washingtonpost.com/wp-dyn/articles/A57330-2000 Jul17.html>$ 

#### Vol #

A speech by White House chief of staff John D. Podesta . . . pleased the business community with the Administration's new software encryption policy, which will loosen export controls on encryption technology, but upset civil libertarians with the Clinton Administration's position on allowing law enforcement agencies to monitor Internet traffic. Barry Steinhardt of the American Civil Liberties Union said the government's attempt to expand wiretapping on the Internet "represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic." (Washington Post 18 Jul 2000)





## 47 Key escrow / recovery laws

2000-02-10 **Keywords:** encryption decryption key legal requirement demand penalties prison law proposal

POLITECH, Slashdot < http://slashdot.org/yro/00/02/09/1445242.shtml >

Vol #

In Britain, controversy erupted over proposals for a new law, The Regulation of Investigatory Powers Bill, that would (among other features) require citizens to hand over their decryption keys if subpoenaed by the Crown. Failure to do so could result in imprisonment. Opponents questioned the consequences of forgetting or losing one's key.





## 48 Foreign crypto & computer crime laws (not cases or sentences)

2000-01-20 **Keywords:** criminal hacker spam spoofing laws legislation police government South China Morning Post

Vol #

In Hong Kong, lawyers with the Department of Justice's Computer Crime Team proposed new laws with criminalization and severe penalties for cybercrime, including spamming, spoofing and unauthorized access to computer systems. Penalties ranged up to 14 years in prison.





2000-01-25 **Keywords:** crypto registration international law regulations

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB948739893578536271.htm >

#### Vol #

encryption.html"

The Chinese government tried to get all foreign companies to register the type of encryption they were using. New rules also forbade Chinese companies from using foreign cryptographic software. Interpreted narrowly, such rules would hamper further development of Internet commerce in that country. However, NewsScan's John Gehl and Suzanne reported, "If everyone covered by China's new regulations on encryption registration had complied, about nine million Internet users would have shown up in one tiny government office to hand-deliver a form specifying what kind of encryption they used on their computers. Instead, only a handful of people showed up. Chinese officials have said there will be no extension of the deadline, but apparently have not yet decided what to do about the companies that missed it -- a group that includes virtually every Chinese and foreign company doing business in China. (Reuters/New York Times 1 Feb 2000) http://www.nytimes.com/library/tech/00/02/biztech/articles/01china-

at mictangerine



# 49 Privacy, consumer profiling, surveillance by law enforcement / govt, legislation, agreements





2000-01-12 **Keywords:** privacy book review study survey overview

EPIC Alert; NetworkWorld Fusion

Vol #

Respected author Simson Garfinkel published his new book, \_Database Nation: The Death of Privacy in the 21st Century and received rave reviews from privacy activists. The Electronic Privacy Information Center (EPIC) published this brief summary in the EPIC Alert 7.01: "Fifty years ago George Orwell imagined a future in which privacy was vanquished by a totalitarian state that used spies and video surveillance to maintain control. In 2000 we find that the threats to our privacy are not coming from a monolithic "Big Brother", but -- even harder to grapple with -hundreds of sources, not seeking to control us, merely to market to us, track us, count us, or streamline paperwork. The result, though, is still as chilling as \_1984\_. \_Database Nation\_ explores the many threats to privacy in the Twenty First century and warns its readers, as Orwell's 1984 did before, that the cost of inaction will be the loss of freedom." The article continued with references to the book's own Web site, < http://www.databasenation.com > . Sandra Gittlen, writing in NetworkWorld Fusion on 2000-03-22, said, "From its first pages, it grips you and makes you realize that the onus for privacy is not just on companies. You, too, have to take some responsibility for how much information you hand out. After all, Garfinkel contends, pretty soon every database could be hooked into every other database, creating a huge Web of information about you." Ralph Nader wrote, "Database Nation by Simson Garfinkel is a graphic and blistering indictment of the burgeoning technologies used by business, government, and others to invade the self -- yourselves -- and restrict both your freedom to participate in power and your freedom from abuses of power. The right of privacy is a constitutionally protected right, and its erosion or destruction undermines democratic society as it generates, in one circumstance after another, a new kind of serfdom. This book is one that you're entitled to take very personally." Peter Neumann of SRI, the moderator of the RISKS Forum, wrote, "You will find this book very much in tune with what you have been reading in RISKS and in Lauren Weinstein's PRIVACY FORUM all these years. Simson has brought it all together very nicely in a highly readable book."





2000-02-28 **Keywords:** communications intelligence COMINT surveillance interception international cooperation

Crypto-gram < http://www.counterpane.com/crypto-gram-9905.html > ; EU Parliament < http://www.iptvreports.mcmail.com/ic2kreport.htm >

Vol 99 # 05

The European Parliament accepted a report on the ECHELON (and other) spy networks in May 1999. See < http://www.iptvreports.mcmail.com/ic2kreport.htm > for the full report. Key findings concerning the state of the art in Comint include:

- \* Comprehensive systems exist to access, intercept and process every important modern form of communications, with few exceptions (section 2, technical annexe);
- \* Contrary to reports in the press, effective "word spotting" search systems automatically to select telephone calls of intelligence interest are not yet available, despite 30 years of research.
- \* However, speaker recognition systems in effect, "voiceprints" have been developed and are deployed to recognise the speech of targeted individuals making international telephone calls;
- \* Recent diplomatic initiatives by the United States government seeking European agreement to the "key escrow" system of cryptography masked intelligence collection requirements, and formed part of a long-term program which has undermined and continues to undermine the communications privacy of non-US nationals, including European governments, companies and citizens:
- \* There is wide-ranging evidence indicating that major governments are routinely utilising communications intelligence to provide commercial advantage to companies and trade.





## 49.1 International agreements

2000-01-12 **Keywords:** international negotiations discussion conflict regulations European Privacy Directive USA

Edupage, Financial Times, EPIC Alert

Vol #

The US government met with European Union officials in mid-January 2000 to discuss the ongoing conflict over the strict EU Privacy Directive. Back on November 15, 1999, the US delegation released the latest in a two-year series of proposals called the Safe Harbor Principles, designed to allay privacy concerns of the Europeans. US negotiators hoped to convince the more government-tolerant Europeans that industry self-regulation would be a reasonable method for protecting citizen privacy.





2000-03-14 **Keywords:** EC European Commission Privacy Directive international agreement Safe Harbor

NewsScan (reprinted with permission), CNet < http://news.cnet.com/news/0-1007-200-1571726.htm>

#### Vol #

The European Union and the U.S. have agreed on regulations covering personal data collected electronically, following months of negotiations aimed at reconciling the disparity in privacy protection laws in the two regions, and giving a boost to trans-Atlantic e-commerce. The new regulations, which require U.S. companies to comply with European rules, are expected to go into effect in June or July. Failure to comply will be considered a deceptive business practice and a prosecutable offense. U.S. companies can cooperate in one of four ways: by reporting to a data authority in Europe, by agreeing to be monitored by U.S. authorities; by joining a self-regulatory body, which will be monitored by the FTC; or by agreeing to rules set by a European panel of data privacy officials. The U.S. Commerce Department will keep a list of industry self-regulators and will provide oversight to ensure they comply with privacy rules. (Bloomberg/CNet 14 Mar 2000)

2000-06-22 **Keywords:** privacy monitoring surveillance organization industry grouping standard protocol P3P

NewsScan (reprinted with permission)

#### Vol #

Though derided by some of its critics as "too little, too late" and as "complex and confusing," a new protocol for protecting individual privacy on the Web has been introduced by the World Wide Web Consortium (W3C), a standards organization, along with AT&T labs, major companies that include IBM, Microsoft and AOL, and the online civil liberties group Center for Democracy and Technology. The new standard, called Platform for Privacy Preferences (P3P), sets standards to allow your browser to automatically read the posted privacy policies of Web sites and alert you before going to any Web site that collects more information about you than you are willing to give. (New York Times 22 Jun 2000)





2000-10-17 **Keywords:** spying eavesdropping industrial espionage network monitoring

international wiretapping artificial intelligence AI lawsuit European

surveillance covert action

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/nb/nb4.htm >

Vol #

[In February, there was news that France would sue the British and US governments over the use of Echelon.] In October, a Green Party member of the European Parliament has filed criminal charges in Germany against "Echelon," the secret international computer surveillance system that monitors most voice and data traffic circulating in Western countries. In 1997 the Covert Action Quarterly, an intelligence newsletter, said: "Unlike many of the electronic spy systems developed during the Cold War, Echelon is designed primarily for non-military targets: governments, organizations, businesses, and individuals in virtually every country. It potentially affects every person communicating between (and sometimes within) countries anywhere in the world." (Newsbytes/USA Today 17 Oct 2000)





## 49.2 EC legislation & regulation





2000-04-14 **Keywords:** data privacy legislation government regulation international EC European Common EU European Union

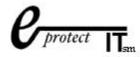
NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB9556575953536545.htm>

#### Vol #

The latest European Union data privacy legislation is in the process of being ratified, and will change the way that companies doing business in Europe collect information on their customers. At issue is the EU's opt-in principle, which requires that each customer give permission for personal data to be shared -- in contrast, the U.S. relies on an opt-out policy, which means personal information can be gathered and passed on unless specifically prohibited by a customer. "Before, processing was authorized unless forbidden," says a lawyer for Belgium's Sabena Airlines. "Now it will be forbidden unless authorized." The EU law also gives individuals the right to correct inaccurate data, to delete any information to which they object, and to collect damages for suffering caused by illegal data processing. A number of U.S. companies are objecting to the new law, saying that little consideration was given to the cost of compliance or the technological feasibility of implementing EU privacy standards. (Wall Street Journal 14 Apr 2000)

[In May,] The European Union . . . passed a landmark e-commerce directive that it hopes will streamline member country decision-making and pave the way for agreement on further initiatives, including ones on copyright, online financial services, and revision of the Brussels convention on contractual law. The new directive spells out rules governing electronic contracts, the information an online merchant must give a customer, what e-mail ads must disclose about the sender, discounts and other promotions, as well as the limits on the liability of intermediaries for unlawful material on their Web sites. Analysts predict that the European e-commerce market will top US\$300 billion by 2003, out of a world total of US\$1.25 trillion. "If we hesitate too long, we will never be able to make up the digital divide, notably with the U.S.," says Frits Bolkestein, internal market commissioner. "Member states need to follow up their words with concrete measures to facilitate the growth of e-commerce." (Financial Times 5 May 2000)





## 49.3 US legislation & regulation

2000-01-13 **Keywords:** privacy government states driving license personal data sale Edupage, Washington Post, EPIC Alert

**Vol** 7 # 01

The Supreme Court of the United States upheld the 1994 Drivers' Privacy Protection Act and refused to allow states to sell drivers' personal information without permission. Several states had opposed the Act because their bureaucrats and politicians saw the sale of drivers' information as a lucrative source of revenue for their governments. Edupage editors wrote, "Privacy and civil liberties advocates reacted with joy yesterday after the Supreme Court decided to uphold the 1994 Driver's Privacy Protection Act, which bars states from selling drivers' personal data without their knowledge. The ruling came as some surprise, as recent court decisions have favored states' authority over such laws. The ruling could establish a precedent that encourages federal lawmakers to pass laws restraining the widespread dissemination of personal data over the Internet, privacy advocates and members of the direct-marketing industry said. In making its decision, the Supreme Court reversed the ruling of the U.S. Court of Appeals for the 4th Circuit, which found the law unconstitutional because it forced states to enforce a federal regulation. The Supreme Court ruled differently, stating that the law `does not require state officials to assist in the enforcement of federal statutes regulating private individuals."





2000-02-24 **Keywords:** privacy law regulation proposal Safe Harbor EC European Commission Data Protection Directive international agreements

NewsScan (reprinted with permission)

Vol #

The Federal Trade Commission . . . [proposed] legislation that will require department stores, automakers, car-rental firms, and other companies to protect the financial privacy of consumers who do business with them. Financial firms will have to create a privacy policy and clear state it to consumers, and give consumers the right to forbid the sharing of their personal financial information with unaffiliated third parties.

\* \* \*

The move by the FTC to impose privacy protection rules on U.S. businesses [was] heralded as a breakthrough by U.S. and European negotiators who have been seeking a way for U.S. firms to do business in Europe without eroding Europeans' privacy rights. In the compromise, the FTC will maintain a list of companies that agree to comply with at least one of four ways of implementing privacy protections: 1) By subjecting themselves to the data-protection authority in one of the 15 EU countries; 2) By showing that they comply with similar U.S. privacy laws; 3) By signing up with a self-regulatory organization such as BBBOnline, which is subject to FTC oversight; or 4) By agreeing to refer privacy disputes to a European regulatory panel. European officials say that resolving the disparities between U.S. and European privacy protections will be key to the success of e-commerce on the continent. (Wall Street Journal 24 Feb 2000)





2000-05-22 **Keywords:** identity anonymity privacy intellectual property copyright infringement policy proposal report think-tank law legislation government

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000522/t000048299.html>

#### Vol #

The Progressive Policy Institute is expected to meet with Congress on Wednesday to deliver its proposed remedy for the current legal wranglings over copyright infringements via the Internet. The changes include: requiring Internet companies to collect personally identifiable and verifiable information from their users, rather than allowing them to sign on anonymously; setting a specific time frame for removing copyright-infringing materials off the Net; and allowing judges to grant injunctions against companies such as Napster whose services are substantially used for exchanging pirated material. (Los Angeles Times 22 May 2000)

2000-06-12 **Keywords:** privacy lawsuit regulation state law prosecution

NewsScan (reprinted with permission). USA Today < http://www.usatoday.com/life/cyber/tech/cti085.htm>

#### Vol #

Michigan Attorney General Jennifer Granholm is threatening lawsuits against four Web sites for failing to tell consumers whether their privacy rights are being protected under state law, even though the sites sold personal products designed for expectant mothers and small children, AIDS patients, sexual voyeurs and stock market investors. "We picked four areas we thought would be of interest and might contain sensitive information. They are examples of how completely inadequate so many privacy policies are." The sites targeted were Johnson & Johnson's www.procrit.com, children's retailer AmericasBaby.com, the voyeuristic Intimate Friends Network and the Stockpoint financial site. (USA Today 12 Jun 2000)





2000-06-20 **Keywords:** privacy law legislation state regulation federal survey

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cti125.htm>

#### Vol #

Internet privacy will be the central topic of the summer meeting of the National Association of Attorneys General, beginning today in Seattle. Citing a recent survey showing that only 20% of the busiest Internet sites offer consumers adequate privacy protections, New York Attorney General Elliott Spitzer sees an opportunity for action at the state level: "There is a void that has been created by the failure of Washington to act. In the absence of any forward movement, it may be time to pursue litigation." (USA Today 20 Jun 2000)

2000-10-03 **Keywords:** privacy opt-in ISP government committee legislation

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/reuters/docs/472958l.htm >

#### Vol #

America Online says consumers certainly should be able to choose to withhold their personal data from being shared among online companies, but urged lawmakers not to change the equation to require that consumers "opt in" -- make an informed decision -- before data collected about them online could be used for purposes other than the transaction at hand. "In the diverse online marketplace, we believe it is impossible to mandate a 'one-size-fits-all' solution to consumer choice," said AOL senior VP George Vradenburg in testimony to the Senate Commerce Committee. Meanwhile, privacy advocates maintain that an "opt-in" system is more in keeping with U.S. notions of civil liberties. "This is the same sort of 'informed consent' system that has become the standard in medicine, banking and other areas," testified Simson Garfinkel, author of "Database Nation: The Death of Privacy in the 21st Century." (Reuters/San Jose Mercury News 3 Oct 2000)





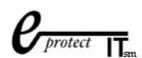
2000-11-29 **Keywords:** privacy corporate policy position officer progress

NewsScan (reprinted with permission), San Jose Mercury News < http://www.mercurycenter.com/svtech/news/breaking/merc/docs/076752.htm >

Vol #

IBM has named Harriet Pearson its first Chief Privacy Officer, responsible for coordinating privacy programs throughout the company. IBM chief executive Lou Gerstner explained: "We know that one of the great conundrums of e-business is that it gives enterprises a powerful new capability to capture and analyze massive amounts of customer information so they can serve individual customers more effectively. Yet this very capability troubles some people, who see it as a means to disclose or exploit their personal information. These are legitimate and very real concerns, and they must be addressed if the world of e-business is to reach its full potential." (Reuters/San Jose Mercury News 29 Nov 2000)





## 49.4 Other legislation & regulation

2000-01-27 **Keywords:** censorship privacy international regulation Internet chat

NewsScan, New York Times <

http://www.nytimes.com/library/tech/00/01/biztech/articles/27china.html >

Vol #

The mainland Chinese government announced yet more of its usual stream of draconian prohibitions against free speech and free thought when it barred anyone from posting "state secrets" on the Internet or via e-mail. A state secret in the People's Republic of China is any information that has not been officially approved for distribution; examples include but are not limited to news of natural disasters, reports of bureaucratic corruption, outbreaks of disease, and worker protests. However, experts predicted that the regulations would ultimately be futile; even now, the sheer volume of e-mail and chat-room communications precludes monitoring more than a tiny percentage of the traffic. As the number of Internet users in China rises, the task will be even greater for the tyrants attempting to control the most popular country in the world.





2000-03-27 **Keywords:** Canada legislation privacy standards enforcement law regulation Government of Canada < http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6\_3/C-6\_cover-E.html >

#### Vol #

In Canada, the Parliament continued consideration of Bill C-6, which Chris Wood described in correspondence published in POLITECH as follows: "a major piece of legislation that will extend Euro-style definitions and obligations of privacy protection to federally regulated businesses and to health providers in Canada. It will also enable e-filing of legal documents . . . and permit (with tech definitions to come) esignatures. It will oblige companies collecting personal data to get informed consent for the collection and allow complaints about abuse of personal information to be submitted for investigation to Canada's Privacy Commissioner."

2000-04-17 **Keywords:** privacy standard proposal

NewsScan (reprinted with permission)

#### Vol #

In April, Microsoft's Director of Corporate Privacy, Richard Purcell, announced that Microsoft would provide free tools to support P3P, the Platform for Privacy Preferences Project. P3P, under development by the World Wide Web Consortium (W3C), allows a browser to signal violation of minimum standards of privacy selected by a user.





### 49.5 Law enforcement

2000-03-09 **Keywords:** law enforcement privacy anonymity accountability investigation NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wpsrv/business/feed/a39970-2000mar9.htm>

#### Vol #

A new Justice Department report, titled "The Electronic Frontier: The Challenge of Unlawful Conduct on the Internet," . . . put privacy activists on alert: "What the report amounts to is a law enforcement Internet wish list of ways in which they can strip away privacy and free-speech protections in order to get at what they claim is this criminal element online," says an ACLU spokeswoman. The most controversial part of the report is a passage that terms anonymous e-mail a "thorny issue": "Given the complexity of this issue, balancing the need for accountability with the need for anonymity may be one of the greatest policy challenges in the years ahead." A White House deputy press secretary attempted to reassure ACLU officials, saying the administration understands the importance of privacy, including the positive role anonymity can play in reporting crimes and war atrocities. (Washington Post 9 Mar 2000)





2000-03-28 **Keywords:** fraud monitoring privacy securities industry government watchdog surveillance controversy

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB954197317969930664.htm>

#### Vol #

An automatic surveillance system that would monitor for online securities fraud is running into trouble before it gets off the ground. The system, which would be operated by the Securities and Exchange Commission, would employ a Web "crawler" to survey public Web sites, message boards and chat groups, looking for key phrases like "get rich quick" and "free stock," and then analyze and index the information for later retrieval by SEC investigators bringing civil proceedings against scam perpetrators. In addition to sparking privacy concerns, the SEC may find itself up against giant Internet operators who consider their chat rooms to be proprietary. AOL, for instance, says it routinely bans outsiders from harvesting information from its chat rooms and message boards, in order to protect its customers' privacy. In addition, the SEC announcement comes at a time when the Federal Trade Commission and many states are working to increase privacy protections for citizens. Congress recently awarded the SEC an additional \$12.5 million this year, primarily for Internet enforcement activities. (Wall Street Journal 28 Mar 2000)





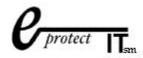
2000-11-07 **Keywords:** privacy keystroke monitoring software forensic logging audit trail investigation

NewsScan (reprinted with permission), TechWeb < http://www.techweb.com/wire/story/TWB20001106S0012 >

#### Vol #

Privacy advocates are concerned about the latest version of WinWhatWhere's Investigator software, which tracks all computer activity, including incoming and outgoing e-mail, both sides of chat room conversations, Instant Message dialogues, Web surfing and all passwords. That information can then be conveyed without the computer user's knowledge to a company's IT administrator, human relations personnel, or even a private investigator. "A lot of things this program does cause me great consternation," says WinWhatWhere president Richard Eaton, who developed the Investigator program. "If you tab across a password field, it picks all that up. I haven't decided if that is good or bad." "It's a complete dragnet," says Beth Givens, director of Privacy Rights Clearinghouse. "Certainly, employees must make personal communications throughout the day, .. and this particular software would pick up those conversations as well. It's certainly ruthless in its pursuit." WinWhatWhere's clients have included major airlines, government agencies, research laboratories, pharmaceutical companies, a large aerospace company, a leading business consulting firm and private individuals. (TechWeb News 6 Nov 2000)





## 49.6 Consumer profiling

2000-01-04 **Keywords:** privacy marketing information leakage software spying lawsuits NewsScan, USA Today < http://www.usatoday.com/life/cyber/tech/cth061.htm >

Vol #

In 1999, RealNetworks management were embarrassed by public outrage over private information about users that was sent discreetly over the Internet by RealJukebox. In January, the company went to court itself demanding relief from lawsuits claiming violation of privacy laws; according to the company attorneys, consumers had agreed to be bound by their licenses for the software. A Seattle judge granted the company a temporary restraining order against the lawsuits.

2000-01-28 **Keywords:** Web privacy identification tracking monitoring shadow spoof restriction access-control

Wall Street Journal, Reuters, Wired

Vol #

Using the IP addresses of visitors to their Web sites, some Webmasters are programming their sites to show different faces to different people. In a kind of weird intrusion-detection mechanism, companies are restricting access so that competitors or known hackers cannot enter. DoubleClick openly admitted that they use cookie-tracking to tailor ads on certain sites so that viewers see a subset based on the sites they previously visited. Many commentators argued that this process violates browsers' privacy, and DoubleClick provided an opt-out feature. Nonetheless, lawyers for Hariett Judnick in California filed suit in January 2000 stating that the company was unlawfully obtaining and selling private information about consumers.





2000-03-03 **Keywords:** consumer privacy compilation data mining targeted advertising marketing ZDNet < http://www.zdnet.com/zdnn/stories/news/0,4586,2428392,00.html > , Los Angeles Times < http://www.latimes.com/business/20000215/t000014627.html>

#### Vol #

DoubleClick got into a public-relations quagmire when it announced in late January 2000 that it would compile information about visitors to numerous Web sites and feed the browsing data to an engine for selection of specific banners ads likely to be more interesting than usual. Many privacy advocates protested that this Abacus Alliance (formed in November 1999) would be too intrusive. DoubleClick executives protested that individual client identification would be protected -- only the shopping and browsing patterns would be stored and used for ad selection.

[In mid-February] DoubleClick [announced] plans to launch a massive ad campaign as part of its "five-point privacy initiative" designed to ameliorate concerns over the advertising firm's online data collection practices. The New York-based company recently was targeted with lawsuits and complaints alleging it violates consumers' privacy by tying Internet users' surfing habits to their names in its massive database. The company also says it plans to hire a "chief privacy officer" and enlist PricewaterhouseCoopers to perform periodic audits of its data collecting procedures. The ad campaign will steer consumers to a new Web site, www.privacychoices.org, which will house information on how the company collects consumer data and how to opt out of that process. Privacy advocates call DoubleClick's efforts too little, too late: "They're launching a major ad campaign because they're trying desperately to avoid legislation," says the director of the Electronic Privacy Information Center, a plaintiff in one of the lawsuits. (Los Angeles Times 15 Feb 2000)

The attorney general of Michigan . . . filed a "notice of intended action" against DoubleClick, charging the Web advertising firm with "failing to disclose to Internet users that DoubleClick is systematically implanting electronic 'cookies,' or electronic surveillance files, on hard drives of users' computers without their knowledge or consent." In addition, the notice criticizes DoubleClick's recent attempts to combine its tracking data with personal data such as names obtained through its acquisition of Abacus Direct last year. Michigan's filing, which is preliminary to a lawsuit, is the third action taken against DoubleClick this week -- the Federal Trade Commission and the New York attorney general earlier launched separate inquiries into the company's business practices. (Financial Times 18 Feb 2000)

The online advertising agency DoubleClick, under pressure from privacy advocates,





has put aside its plan to integrate the anonymous data it collects about consumer online purchasing patterns with personal information about millions of consumers in the databases of Abacus Direct Corporation, a company DoubleClick purchased last year. DoubleClick chief executive Kevin O'Connor says, "I made a big mistake. It was wrong to try to match that information in the absence of industry or government standards, so until that there's agreement on it, will not... Now we're just happy to get this behind us and move on." (New York Times 3 Mar 2000)

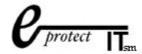
2000-03-16 **Keywords:** privacy children monitoring inference inquiry prediction banner advertisement consumer profiling advice

NewsScan (reprinted with permission)

Vol #

E-tractions, a Bedford, Mass. sells online quizzes and games to Web companies that want to jazz up their sites, but their games do more than entertain. E-tractions GameServer software analyzes the quiz-takers' answers to learn more information about them in order to target them with ads or steer them toward other parts of the site. For instance, on WebHire's site, an "HR IQ" test under development will poll readers on their experience with various employment issues, and then the company will offer them products based on their answers. A game under development for the upcoming MsMoney.com site will poll girls on the cost of items in a "Price is Right" - type game, quiz them on the type of lifestyle they'd like to have, and then counsel them on the type of job they will need to support that lifestyle. "If you want a BMW and to live in the Marina district, you'll need an engineering degree and a Stanford MBA," says MsMoney.com's CEO. (Wall Street Journal 16 Mar 2000)





2000-03-31 **Keywords:** Web privacy consumer profiling FTC investigation NewsScan (reprinted with permission)

Vol #

Yahoo Inc. has notified the Securities and Exchange Commission that it had volunteered to cooperate with an inquiry by the Federal Trade Commission into how Web sites gather and use personal information. Insisting that it takes its privacy policies seriously, the company says that the discussions have "nothing to do with advertising profiling" but has declined to elaborate on the scope of those discussions. Most Web sites gather personal data about their visitors not to collect information about individuals but to determine broad demographic characteristics that will attract advertisers who want to target their messages to prescreened audiences. (New York Times 31 Mar 2000)

2000-04-16 **Keywords:** data privacy children kids identification

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/ap/docs/432874l.htm>

Vol #

Eric Shen, a policy analyst with the Electronic Privacy Information Center in the capitol, calls the new federal privacy law requiring that Web sites get parental permission before collecting personal information on kids, is "a serious first step" but says it also has a serious defect, because sites can evade the law merely by not asking hold old users are. But Mozelle Thompson of the Federal Trade Commission argues: "Sure, there are ways around it. But that doesn't mean you don't put a few speed bumps in." (AP/San Jose Mercury News 16 Apr 2000)





2000-05-01 **Keywords:** Web consumer data behavior profiling marketing banner advertisements privacy

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB957139612628916016.htm>

#### Vol #

Predictive Networks Inc., a Web company opening its doors today, began drawing protests among privacy advocates well before its launch. Predictive has developed software that can track every site a Web surfer visits and then build a profile of him. Based on the profile, Predictive automatically sends ads targeting his interests. Predictive believes that surfers are willing to give up some privacy in exchange for free Internet access, and advertisers are already coughing up ad rates as much as six times higher than usual for the service. But privacy advocates caution that the technology pushes the depth of digital eavesdropping to a new level. "It takes a court order and tight supervision to listen over a telephone link," says one. "It's really time for Congress to set limits and decide that we need a privacy policy." (The Wall Street Journal 1 May 2000)





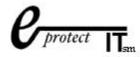
2000-05-08 **Keywords:** consumer profiling Web privacy e-commerce

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000508/t000043365.html>

Vol #

If you buy event tickets online, you'll have noticed an increase in associated merchandise and memorabilia offered by the ticketseller at the same time. Online ticketing companies like Ticketmaster's Internet partner and Tickets.com are scrambling to come up with new revenues over and above the price of the tickets to offset the 20% to 50% more it costs them to sell electronically rather than through traditional channels. Ultimately, online ticketers say their services will lead to increased convenience for customers and a profitable bottom line, but right now, they're struggling to cover hefty marketing, infrastructure and customer service expenditures. Ticketmaster Online-CitySearch lost more than \$121 million last year, and Tickets.com recorded losses of \$66.6 million. Meanwhile, ticketsellers are reaping the benefits of a new resource -- more information about their customers. By requiring a bit of demographic data from would-be buyers, they're building valuable databases. "One of the realities about Springsteen is that 200,000 people will try to buy tickets when we only have 20,000 seats," says Ticketmaster.com president Tom Stockham. "We used to know nothing about 180,000 of those people." (Los Angeles Times 8 May 2000)





2000-06-07 **Keywords:** privacy consortium industry self-regulation organization consortium NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000607/t000053796>

#### Vol #

A seven-member coalition of leading high-tech companies . . . [proposed] a new system aimed at protecting consumers from online fraud and privacy intrusions in cyberspace. The group, which includes America Online, AT&T, Dell, IBM and Microsoft, has developed voluntary guidelines that would require merchants to clearly spell out the terms and conditions of a sale, make reasonable efforts to protect consumer privacy, and provide for "fair, timely and affordable" dispute resolution. The move is seen as a strategy to allay consumers' fears and ward off further intervention by government regulators at a time when the Federal Trade Commission is pushing for expanded powers to regulate industry Web sites, and several bills in Congress seek to increase consumer protections against cyberscams and privacy abuses. Although . . . [fewer] than 20% of Web sites post privacy policies, polls have found that privacy is the No. 1 concern of online users. (Los Angeles Times 7 Jun 2000)

2000-06-22 **Keywords:** privacy cookies government Web policy politics NewsScan (reprinted with permission), USA Today

< http://www.usatoday.com/life/cyber/tech/cti139.htm>

#### Vol #

The Clinton Administration's Office of National Drug Control Policy . . . [was] criticized by Republican lawmakers for using "cookies" (small programs placed surreptitiously on a Web-user's computer) to track the individual's subsequent journey through the Web. House Majority Leader Dick Armey (R., TX) said: "'The government should not be in the business of cybersnooping... It is an outrage when this vital trust is violated by the lack of concern for personal privacy.'' The drug office says it will stop using cookies. (AP/USA Today 22 Jun 2000)





2000-07-20 **Keywords:** cookies privacy monitoring consumer profiling Web software countermeasures

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/internet/docs/218367l.htm>

#### Vol #

Microsoft is about to begin testing new software to allow users of its Internet Explorer software to receive alerts when there is an attempt to place "cookies" on their hard disks by Web sites they visit. Cookie trails are used by many sites to follow the travels of Web surfers in order to provide them with personalized content and/or targeted advertising. The new Microsoft software, which will be released to the public for beta testing within the next month, is also intended to give consumers an easy way to manage and delete cookies. (Reuters/San Jose Mercury News 20 Jul 2000)

2000-08-15 **Keywords:** I&A identification & authentication token monitoring

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/library/financial/columns/081600tv-adcol.html>

#### Vol #

A new system called Whispercode, designed by a New Jersey company for monitoring the effectiveness of TV advertising, will involve the encoding of commercials with inaudible, identifying signals that can be picked up by a small device worn by a participant (perhaps in a bracelet or keychain) and relayed to a nearby recording box that records the fact that the wearer was in the room when the commercial was broadcast. [It should be noted, though, the system can't detect whether the participant is awake, attentive, and not bored to death.] The company's chief executive officer says, "With Whispercode, we will finally be providing our clients with a true accounting of where their advertising money is going." (New York Times 15 Aug 2000)





2000-08-15 **Keywords:** privacy monitoring Web cookies lawsuit consumer profiling NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/articles/A25494-2000Aug14.html>

#### Vol #

The Boston technology company Pharmatrak is able to use "cookies" to surreptitiously track the movements on the Web of visitors to the sites of various pharmaceutical companies, and, because it is not an advertiser, is not bound by a recent agreement by such online advertisers as DoubleClick and Engage to allow computer users to choose whether or not they wish to allow their activities on the Web to be monitored. Threatening the possibility of legal action against Pharmatrak, Michigan's attorney general . . . [said], "They've taken stealth to a new low... It's a classic example of corporate surveillance. There's no way your average computer user has any idea." Pharmatrak says it doesn't collect the names of individuals, and has no intention of doing so, and Pharmatrak's chief executive says of the lawsuit threatened by Michigan: "If they file a suit like that they're idiots," because people know or ought to know that "they're using an open access means of communication." (Washington Post 15 Aug 2000)

2000-08-30 **Keywords:** surveillance monitoring positioning chip mobile phone NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/reuters/docs/356409l.htm>

#### Vol #

The Irish chip designer Parthus Technologies has developed a product called NavStream, based on the Global Positioning System (GPS), that will be able to identify the location of a mobile phone user to within five yards. That kind of capability would allow the creation of various new location-sensitive information services, including emergency assistance calls. A company executive adds: "Parents can keep track of their children's exact location by embedding GPS technology into a watch or other device, giving them peace of mind." (Reuters/San Jose Mercury News/30 Aug 2000)





2000-10-02 **Keywords:** e-commerce ethics marketing pricing consumer tracking profiling privacy NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20001002/t000093531.html>

#### Vol #

Although it's proven a public relations debacle for Amazon, industry analysts say that the "dynamic pricing" model recently tested by the online merchant could spread to other e-tail operations. "Dynamic pricing is the new reality, and it's going to be used by more and more retailers," says one Internet consultant. "In the future, what you pay will be determined by where you live and who you are. It's unfair, but that doesn't mean it's not going to happen." What's especially troubling about the Amazon test, say some customers, is that regular customers were being charged more than new visitors for the same item. "This is a very strange business model, to charge customers more when they buy more or come back to the site more," says a message posted to the DVDTalk.com message board, where participants recently discerned Amazon's new pricing practice. "This is definitely not going to earn customer loyalty." (Los Angeles Times 2 Oct 2000)





# 49.7 Trade in personal information

2000-01-28 **Keywords:** privacy consumer information lawsuit

NewsScan, ZDNet < http://212.187.198.142/news/1999/51/ns-12357.html >

Vol #

On 30 Dec 1999, Universal Image Inc. sued Yahoo! for breach of contract, claiming that when Yahoo! bought a company called Broadcast.com, the new owners reduced the flow of customer information to Universal Image. The plaintiffs demanded \$1B in damages and \$3B in punitive damages. The judge agreed to issue a preliminary injunction to prevent Yahoo! from publishing its own privacy policy, which allows users to determine how much information about them can be shared with other companies; Universal objected to this stance, saying that the information was valuable and ought to be turned over to them, presumably regardless of the data subjects' opinions. The judge in the case later ruled that the companies would have to go to arbitration. However, in a surprising development, Universal turned around and accused Yahoo! of violating consumer rights by using cookies on its Web site. Such use, claimed the plaintiffs piously (and ignoring their previous stance \_against\_ consumer privacy) violated Texas anti-stalking laws. In a separate action, Universal Image's attorneys threatened to launch a class-action suit on behalf of aggrieved consumers.





2000-02-01 **Keywords:** privacy Web health consumer visitor e-mail data sharing conversion NewsScan (reprinted with permission),

< http://www.sjmercury.com/svtech/news/breaking/internet/docs/160309l.htm>

Vol #

In a study conducted for the California HealthCare Foundation, the Georgetown University's Health Privacy Project has found that drkoop.com, webmd.com, ivillage.com, yahoo.com, onhealth.com, and other Web sites that provide information on health matters are cavalier about privacy practices: "The privacy policies of health Web sites do not match up with their own practices." Example: some companies share e-mail addresses and other visitor data even though their Web sites promised they would do no such thing. The companies are disputing the study findings. (Reuters/San Joe Mercury News 1 Feb 2000)

2000-03-21 **Keywords:** privacy social security number SSN auction lawsuit

**RISKS** 

Vol 20 # 85

The well-known actor Jerry Orbach (best known for his role in the TV show "Law and Order") discovered that someone sold two old contracts he had signed. Unfortunately, the scanned images showed his Social Security Number and apparently led to credit-card fraud in his name. He sued eBay, where the electronic auction took place.





2000-03-31 **Keywords:** privacy lawsuit consumer tracking Web usage profiling NewsScan (reprinted with permission), http://www.latimes.com/wires/20000208/tCB00V0164.html

#### Vol #

[In February,] Amazon.com executives . . . [told] the U.S. Securities and Exchange Commission that there is "no merit" in lawsuits filed against an Amazon subsidiary, the software company Alexa Internet. The Federal Trade Commission is conducting an "informal" investigation of claims made against that company alleging that Alexa's software for tracking Web usage secretly intercepts personal data, which it then resends to Amazon and other third parties. Security consultant Richard Smith, who is the one who originally raised the issue of possible privacy violations, says that since some Web addresses may contain personal information such as mailing addresses or customer account numbers, it is "conceivable" that something like Alexa could tie the information with a customer's surfing patterns and create a profile. Alexa executive Dia Cheney says, however, that Web usage patterns and customer data are stored in separate databases that are not linked.

[In March,] Meanwhile, Amazon . . . [said] the FTC . . . [had] opened a formal investigation into the e-tailer's Alexa Internet software division, which tracks Internet users as they navigate Web sites in order to suggest other things they might be interested in viewing. . . . The FTC investigation will focus on whether the division engaged in "unfair or deceptive acts." (Seattle Times 31 Mar 2000)





2000-05-12 **Keywords:** privacy anonymity lawsuit Internet service provider ISP employer employee firing subpoena

NewsScan (reprinted with permission)

Vol #

An Internet user who posted disparaging remarks about his bosses on a Yahoo stock market message board . . . filed a lawsuit accusing Yahoo of violating his right to privacy after the Internet portal revealed his identity to his employer, who then promptly fired him. Although AOL settled a similar lawsuit in 1998 after it revealed to U.S. Navy officials the identity of an officer who'd disclosed in an anonymous chat room that he was gay, the Yahoo lawsuit addresses what's become a far more pervasive problem: the anonymity of Internet users who post messages on stock market message boards. Many companies argue that the postings can sometimes be libelous, untrue and designed to drive stock prices down. A frequent tactic used by these aggrieved companies to identify authors of libelous material has been to file a "John Doe" lawsuit, and then subpoen the message board sponsor for the real identity of the message poster. The suits are usually dropped after the identity is turned over. Privacy advocates complain that many Internet companies sponsoring message boards tend to cave in without scrutinizing the legal basis for the "John Doe" suit, and do not adequately warn users before they turn over their information. (Los Angeles Times 12 May 2000)





2000-07-11 **Keywords:** privacy intellectual property IP bankruptcy asset

NewsScan (reprinted with permission), New York Times < http://www.nytimes.com/library/tech/00/07/biztech/articles/11toysmart.html>

#### Vol #

Toysmart, the now-defunct online toy retailer partly owned by the Walt Disney Co., . . [was] accused by the Federal Trade Commission of violating its own consumer privacy assurances by selling off, as one of its assets, a database that contains consumer names, addresses, and family profiles, including the names and ages of children. FTC official David Medine . . . [said], "As a shakeout of dot-com companies occur, they can't sell out customer lists they promised to protect like they do other assets, like paper clips or computer equipment." (New York Times 11 Jul 2000)

2000-09-25 **Keywords:** consumer privacy amalgamation Web tracking profiling inference databases concerns worries commerce

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/thestreet/business/1095666.html>

#### Vol #

Online advertiser DoubleClick is acquiring @plan.inc, a Web market research company that offers clients such as eBay, Microsoft, and CNN Interactive analyses of customer lifestyle issues, product preferences, and demographic profiles. The combined company client base will boast more than 6,000 ad agencies, advertisers, and Web publishers. (New York Times 25 Sep 2000)





2000-12-04 **Keywords:** privacy personal information traffic ownership asset criticism policy NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cti873.htm >

#### Vol #

Two privacy groups, Junkbusters and the Electronic Privacy Information Center, . . . [wrote] to the Federal Trade Commission complaining about online retailer Amazon.com's revised privacy policy specifying that information about its customers is a company asset that can be sold if the company were to go out of business or sell a division. Amazon insists that the policy protects all customers by indicating when the company may or may not share data. (AP/USA Today 4 Dec 2000)

2000-12-19 **Keywords:** personal information privacy abuse traffic violation study research NewsScan (reprinted with permission), Information Week < http://www.techweb.com/wire/story/TWB20001219S0010 >

#### Vol #

In the world of struggling Internet startups, sometimes the data they've collected on their customers turns out to be their most valuable asset. "Data is worth a lot of money," says a Forrester Research analyst, and therefore "the incentive for startups to violate privacy is strong." Even the biggies -- DoubleClick and Amazon -- face alleged consumer privacy breaches, and the fear is that online companies' cavalier attitudes will create a consumer backlash. Forrester estimates that privacy fears will cost online retailers \$12.4 billion in sales this year, and predicts that when Congress reconvenes next year, consumer privacy legislation will be high on the agenda, because it is a bipartisan issue that affects everyone. (InformationWeek 19 Dec 2000)





# 49.8 Anonymity

2000-03-31 **Keywords:** anonymity DNS Domain Name Service registration owners privacy POLITECH, FTC < http://www.ftc.gov/os/1999/9910/icann.htm >

Vol #

One of the comments to ICANN (the Internet Corporation for Assigned Names and Numbers) on proposals for enforcing valid names, addresses and phone numbers in DNS (Domain Name Service) registration came from the FTC. The Staff of the Bureau of Consumer Protection of the Federal Trade Commission wrote (as quoted by Declan McCullagh in POLITECH), "We support those measures contained in the Tentative Agreements which are aimed at improving the accuracy of registration contact information, and offer two suggestions for closing possible loopholes in those measures. The first recommends domain name suspension in situations where a registrar is unable to obtain accurate contact information after a reasonable investigation. The second encourages ICANN to avoid delay in adopting a policy requiring registrars to implement reasonable verification procedures. . . . For law enforcers working to prevent Internet fraud, the problem of false domain name registration information has become an impediment to effectively identifying law violators. When accurate, the registration information publicly available on the Whois database provides an important tool for tracking down the operators of Web sites violating the law. Commission investigations are increasingly being hampered, however, by registration information that is not only false, but sometimes clearly false on its face. . . . Commission staff also supports the requirement in paragraph II(F)(1) of the Accreditation Agreement that a registrar make publicly available the essential contact information in real-time.





2000-06-09 **Keywords:** anonymity libel subpoena court ruling judgement

NewsScan (reprinted with permission), New York Times

< http://partners.nytimes.com/library/tech/00/06/cyber/cyberlaw/09law.html >

#### Vol #

In Florida's Miami-Date County Circuit Court, Judge Eleanor Schockett . . . ruled that someone making libelous statements cannot post them on the Internet and count on having the Internet service providers keep their identity secret. Ordering Yahoo and AOL to comply with a civil subpoena requiring them to reveal the real names of persons accused of libel, the judge rejected First Amendment arguments made by a lawyer for the defendants. (New York Times 9 Jun 2000)

2000-08-07 **Keywords:** industrial espionage sabotage trade secrets employee lawsuit anonymity

identity free speech Internet service provider ISP ruling judgement

subpoena anonymity

NewsScan (reprinted with permission), USA Today

< http://www.usatoday.com/life/cyber/tech/cti346.htm>

#### Vol #

In response to a complaint from Apple that an unidentified person using the alias "worker bee" violated the company's trade secrets by using the GeoCities site to post information about new Apple products before their official announcement, a Superior Court judge in California has ordered GeoCities (a division of Yahoo!) to yield the person's name, e-mail and street addresses, phone number, and Internet Protocol address. First Amendment rights advocates believe that anonymous message-writers should be able to conceal their identifies unless it has been shown that they've violated the law. But Apple says that only someone who illegally violated the company's nondisclosure agreement could have made the posting it finds objectionable.





2000-11-29 **Keywords:** anonymity libel breach confidentiality intellectual property lawsuit judgement ruling sabotage

NewsScan (reprinted with permission), San Jose Mercury News < http://partners.nytimes.com/2000/11/30/technology/30COMP.html >

#### Vol #

A Superior Court judge in New Jersey . . . ruled against Dendrite International's attempt to force Internet portal Yahoo to reveal the names of three individuals who, using the names like "ajcazz" and "xxplrr," allegedly libeled the company and revealed company secrets. An attorney for the consumer advocacy group Public Citizen called the ruling "a tremendous victory for free speech." (AP/San Jose Mercury News 29 Nov 2000)

2000-12-15 **Keywords:** anonymity libel court ruling judgement

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/2000/12/14/technology/15CYBERLAW.html >

#### Vol #

Last week a federal judge in Virginia approved a \$675,000 jury award to a doctor libeled in an anonymous posting on a Yahoo bulletin board. University of Florida law professor Lyrissa Barnett Lidsky explains: "What this case demonstrates is that people can be held accountable for what they post on the Net even though they posted anonymously. People need to understand that if they make an allegation of fact about someone online that is damaging to that person's reputation, they better make sure that statement is true; otherwise they can be held liable for libel." (New York Times 15 Dec 2000)





# 49.9 Industry efforts

2000-06-21 **Keywords:** privacy consortium alliance industry grouping corporations surveillance monitoring

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/ap/docs/120261l.htm>

# Vol #

The "Oxygen Alliance," a \$50-million MIT research project to make computers as ubiquitous and invisible as oxygen, has received funding from the Defense Department and a group of corporate sponsors that includes Acer, Delta Electronics, Hewlett-Packard, NTT, Nokia, and Philips. Computers would be embedded everywhere, in common objects, networked together though sensors, microphones and cameras, manipulated by handheld devices with features of cellphones, handheld computers, radios, and remote controls. The project leaders note that some privacy issues are yet to be resolved, and one of them says: "How do we feel about having microphones listening to what we're saying, and cameras looking at what we're doing?" (AP/San Jose Mercury News 21 Jun 2000)

2000-07-25 **Keywords:** privacy education campaign publicity organization consortium alliance NewsScan (reprinted with permission)

#### Vol #

Thirty-six information technology companies, including AOL, IBM, Intel, Microsoft, RealNetworks, and Verizon, . . . [joined] in the public education campaign Privacy Partnership 2000, which will use print, radio, and Web advertising to explain to the public the importance of respect for individual privacy on the Internet. The campaign will point consumers to privacy education pages on the Web site TRUSTe, www.truste.com. (AP/San Jose Mercury News 25 Jul 2000)





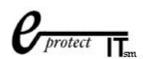
2000-07-26 **Keywords:** privacy organization education monitoring surveillance

NewsScan (reprinted with permission), New York Times < http://www.nytimes.com/library/tech/00/07/biztech/articles/26cyber.html>

Vol #

A new Denver-based group called the Privacy Center will gather data on whether and how personal information is captured by software makers and Internet service providers and merchants. Richard M. Smith, the well-known software engineer who helped track down the origins of various computer viruses, is the organization's chief technology officer. Smith explains: "We'll look at anything to do with a computer, and stuff that is networked together. We'll focus on how we're being monitored in our daily lives." (New York Times 26 Jul 2000)





# 4A2 Pointing, linking

2000-03-09 **Keywords:** trademark lawsuit Web banner advertisements focus profile NewsScan (reprinted with permission)

Vol

Cosmetics giant Estee Lauder has won a lawsuit filed in Germany against Excite Inc. and New York-based iBeauty, with a Hamburg District Court agreeing that Excite's sale to iBeauty of certain Estee Lauder trademarks, such as Estee Lauder, Clinique and Origins, amounted to unfair competition under German law. The trademarks were used by the companies to trigger banner ads for [other] beauty products on Web sites. Similar lawsuits have been filed by Estee Lauder in federal court in New York and in France. A Jupiter Communications analyst says the case "has major implications for many sites across the Web," because keyword-based ads generate hundreds of millions of dollars in revenue. He calls the German decision "at least a first precedent out there in cyberspace related to this type of conflict." (Wall Street Journal 9 Mar 2000)





2000-03-29 **Keywords:** Web linking pointing legality lawsuit judgement

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000329/t000029415.html>

Vol #

A federal judge has ruled that it is not illegal for an online company to provide a link on its Web site to that of a competitor. The ruling came in response to a lawsuit filed by Ticketmaster Online-CitySearch against Tickets.com. In dismissing four counts of Ticketmaster's lawsuit, the judge said that "deep linking by itself... does not necessarily involve unfair competition," as long as it is clear whose site a customer is on when they click through. Ticketmaster says it will file an amended complaint and attempt to reinstate the dismissed charges. "If we spend substantial money to build up a site why should they be able to take that and build their business on the backs of our hard work?" says Ticketmaster attorney Robert Platt. Tickets.com attorney Daniel Harris replies, "They have an open site and are a member of the free Internet community. They have to live by the rules of that community as it has grown up." (Los Angeles Times 29 Mar 2000)

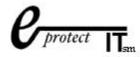
2000-04-10 **Keywords:** linking legal judgement lawsuit

**POLITECH** 

Vol #

In Osaka, Japan, a court ruled against the creator of the FLMASK utility software that allows users to remove the anti-porn digital masks from films. The judge also ruled that all sites linking to the offending URL were in violation of the law.





2000-05-09 **Keywords:** free speech linking legislation proposal Wired < http://www.wired.com/news/politics/0,1283,36209,00.html >

Vol #

The Methamphetamine Anti-Proliferation Act proposed in Congress would have made it a federal crime to link to any information about illegal drugs or to advertising for illegal drugs. The proposal suffered widespread condemnation for violation of US First Amendment guarantees and vagueness.

2000-05-13 **Keywords:** linking free speech lawsuit

**POLITECH** 

Vol #

Microsoft sent demands to Slashdot insisting that it not only remove objectionable articles but also links to specific sites containing copies of material claimed to be in violation of Microsoft's copyrights.





2000-06-06 **Keywords:** Web pointing lawsuit principle fundamental

NewsScan (reprinted with permission)

Vol #

MP3Board Inc. . . . [sued] the Recording Industry Association of America in an effort to avoid having its mp3board.com Web site, which includes a search engine and hyperlinks to other sites, shut down. Since October the RIAA has been writing cease-and-desist letters to MP3Board, claiming "that mere hyperlinks to other works on other sites was a copyright infringement." MP3Board's suit "seeks to declare that hypertext linking, created by automated processes, from one site on the World Wide Web to another does not constitute copyright infringement even if the destination of the hypertext link is to a Web site containing material that infringes upon intellectual property rights." A review of the mp3board.com site by the RIAA found at least 662 links that it believes are infringing on the copyrights of the five major record labels it represents. (Hollywood Reporter 6 Jun 2000)





# 4A3 Jurisdiction

2000-02-22 **Keywords:** jurisdiction online gambling fraud

NewsScan (reprinted with permission)

Vol #

In a New York trial that's testing whether this country's. criminal laws apply to Web sites beyond U.S. borders, 21 defendants are charged with using the Internet to violate a law that provides for sentences of up to five years in prison and \$250,000 in fines for placing or taking bets over phone lines. The gambling site (based in Antigua, where Internet gambling is legal) accepted bets placed through the Web by U.S. citizens. One of the defendants insists: "As far as we're concerned, all bets are placed here on our server here in Antigua, which is a sovereign state and we're fully licensed"; however, Washington lawyer Jim Halpert comments: "It may not make a difference whether the server was located in Antigua, because the federal anti-gambling law in question applies broadly. Typically, the fact that a site is doing business with consumers in a jurisdiction is sufficient to establish jurisdiction in the state where the consumer is located." (USA Today 22 Feb 2000)





2000-06-04 **Keywords:** criminal hacking privacy data haven monitoring government sovereignty jurisdiction

NewsScan (reprinted with permission), New York Times < http://partners.nytimes.com/library/tech/00/06/biztech/articles/04have.htm>

#### Vol #

A company called Havenco has built what it calls a "data haven" on an abandoned military platform in the sea, six miles off Britain's coast, in order to offer communications services to clients who want to avoid monitoring by governmental authorities. Declaring his small fortress a sovereign country beyond the reach of British law, Havenco co-founder and chief executive Sean Hastings, a 32-year-old U.S. citizen, says, "Technology has made it easier to move information and hide information. Soon it will be impossible to trace where money is and who has money, and that will eventually force governments to move away from income taxes and toward consumption taxes." (New York Times 4 Jun 2000)

2000-10-11 **Keywords:** extortion theft fencing law enforcement police international jurisdiction NewsScan (reprinted with permission), MSNBC < http://www.msnbc.com/news/475316.asp >

#### Vol #

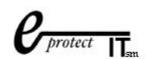
A Web site devoted to the sale of stolen goods has raised the ire of British lawmakers, who point out that it is illegal to sell stolen property back to its owner. TheBurglar.com is accused of violating the Theft Act by charging people "reward" money for the return of their possessions. Victims of burglaries can post the details of their losses on the site, and burglars are then invited to anonymously contact their victims by e-mail to negotiate the return of the stolen property. The site collects the agreed-upon cash, and keeps it until the victim has verified receipt of the goods. TheBurglar.com then sends the payment to the address or account of the thief's choice. And despite outrage among law enforcement officials, TheBurglar.com likely will escape prosecution. A note on its site reads: "TheBurglar.com Headquarter is placed in Copenhagen, but due to spite we have moved the office to a secret location." (ZDNet UK 11 Oct 2000)





# 4A4 Blocking





2000-05-25 **Keywords:** autonomous agents crawlers bots contract law commerce restrictions property auction

NewsScan (reprinted with permission), WSJ

- < http://interactive.wsj.com/articles/SB955937300461505269.htm> , San Jose Mercury News
- < http://www.sjmercury.com/svtech/news/breaking/ap/docs/36278l.htm>

#### Vol #

The Justice Department is investigating whether eBay's block on "shopping bots" and "crawlers" constitutes anticompetitive behavior. At issue are software programs used by two aggregator sites that compile lists of thousands of sales across a number of auction sites. Bidder's Edge and AuctionWatch have been meeting with Justice officials to discuss the filtering actions taken by eBay that block their ability to search its site. EBay does allow shopping bots from other sites to search its database, but only after they sign a licensing agreement to do so. It has called unauthorized listings of its wares "trespassing and stealing," but Bidder's Edge CEO James Carney says, "What's at stake here is the architecture of commerce on the Internet, whether you can freely search others' sites or whether you have to have their permission. (EBay's tactics) threaten to break down the openness that made the Internet great." (Wall Street Journal 4 Feb 2000)

[In April,] A federal judge . . . [said he was] planning to issue an injunction against Bidder's Edge, one of several so-called aggregators of online auction listings that compile and compare information on eBay, Yahoo, Amazon and other auction operators. The ruling comes in response to a lawsuit filed by eBay, which charges that Bidder's Edge violated the federal Computer Fraud and Abuse Act by using information gleaned from eBay's site. Legal scholars say such a ruling could set new standards in a debate over what is considered copyrightable intellectual property. "Decisions like this are disturbing because if extracting information off a site like eBay's is trespass, then it's going to be difficult for consumers to have the benefit of services that do price comparisons," says a University of California, Berkeley law professor. (Wall Street Journal 17 Apr 2000)

[In May,] Saying that the law recognizes no right to use another's personal property, U.S. District Judge Ronald Whyte . . . ruled that the Internet firm Bidder's Edge trespassed against auction firm eBay when it used "spider" software to crawl through eBay's Web site acquiring information that had been amassed by eBay. Bidder's Edge . . [claimed] that the issue is "about the openness of information on the Internet," but eBay argues that the judge's ruling was "important for all Internet entrepreneurs who hope to create businesses based on databases without fear that trespasses will come in and steal the fruits of their labor." (AP/San Jose Mercury News 25 May 2000)









# 4B1 Copyright

2000-01-29 **Keywords:** intellectual property confidentiality source code DVD lawsuit error evidence documents

**RISKS** 

**Vol** 20 # 77

In filing documents with the court in the DVD industry's lawsuit against the authors of the DeCSS decoding software, attorneys for the DVD Copy Control Association forgot to ask the judge to prevent disclosure of the industry's encryption source code. The materials were distributed on the Web before the judge sealed the evidence.





2000-02-09 **Keywords:** copyright lawsuit Canada theft Web intellectual property international boundary jurisdiction

 $News Scan, USA\ Today < \ http://www.usatoday.com/life/cyber/tech/cth190.htm > , San\ Jose \\ Mercury\ Times < http://www.sjmercury.com/svtech/news/breaking/ap/docs/188993l.htm >$ 

#### Vol #

A Canadian Web site, iCraveTV, was sued by a consortium of broadcasters and film owners for posting their intellectual property without license. The owners of iCraveTV retorted that Canadian law does not forbid such piracy. The CRTC (the Canadian equivalent of the US Federal Communications Commission) declined to intervene in the case. A federal judge granted the plaintiffs a temporary restraining injunction to stop the video pirates from further use of unlicensed materials.

[On 9 February, ]A U.S. federal judge has issued a 90-day injunction against continued operation of the Toronto-based Web site iCraveTV, which captures TV programs from stations in Toronto and Buffalo and rebroadcast them live (along with new ads sold by iCraveTV) to Canadians. The company's founder takes the position that such activity is permissible under Canadian law, and that iCraveTV will reinforce its security mechanisms to make sure that the rebroadcasts would not be viewable south of the U.S.-Canadian border, and that the company would meet industry standards. But an executive of the Motion Picture Association of America protests: "There is no acceptable industry standard for piracy." (AP/San Jose Mercury News 9 Feb 2000)





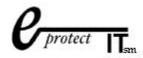
2000-04-14 **Keywords:** copyright intellectual property ISP Internet service provider court legal lawsuit common carrier

NewsScan (reprinted with permission)

Vol #

Internet service providers in Germany . . . [were] facing a new legal challenge after a Munich court found AOL Europe liable for damages resulting from the downloading of copyrighted music via an online forum. The court's decision is reminiscent of the 1998 ruling that found Felix Somm, former head of CompuServe in Germany, guilty of failing to block access to child pornography. That ruling triggered widespread criticism and was overturned last year. AOL Europe says it had fulfilled its legal obligations and had made a good faith effort to discourage copyright violations by its subscribers. "We are only the messenger," says an AOL spokesman. "Nobody would have sued the Royal Mail or Deutsche Post for delivering a package that contained illegal CDs." Damages have not yet been set, and AOL is considering an appeal. If the Munich verdict is upheld by a higher court, "then the online industry has a major problem," says one industry observer. (Financial Times 14 Apr 2000)





2000-05-15 **Keywords:** intellectual property compilation copyright lawsuit

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB958348989291026253.htm>

#### Vol #

Upstart Jurisline.com . . . [was] sued by legal publisher Lexis for copying the CDs containing court opinions and related documents that Lexis sells and distributing the same information free on its Web site. For decades, the database of legal material has been marketed by two companies -- Reed Elsevier's Lexis and Thomson Corp.'s West Publishing -- which charge premium rates for access to a single document and reap millions of dollars a year in subscription fees from the nation's law firms. Jurisline.com, on the other hand, distributes the information for free, making its revenue on advertising. At issue in the court case is whether Lexis's license agreement prohibiting the purchaser from developing "a database, infobase or other information resource" is legally enforceable, given that the materials in question were written on the taxpayer's dime and can't be copyrighted. . . . (Wall Street Journal 15 May 2000)





2000-06-28 **Keywords:** intellectual property encryption value-added network

NewsScan (reprinted with permission), New York Times

< http://partners.nytimes.com/library/tech/00/06/biztech/articles/28online.html>

#### Vol #

In a move that could help diffuse the controversy surrounding the downloading of digital music, America Online says it is teaming up with InterTrust to promote its encryption software in AOL's version 6.0 CDs, to be distributed later this year. The InterTrust system enables a recording company to surround a digital music file with software that ensures it will only be played according to rules specified by the company. In addition, AOL will integrate InterTrust's system into a version of its Winamp music player, a move that could boost Winamp's popularity among companies seeking to distribute digital music. "We could be at the threshold of something very big," says Talal Shamoon, senior VP for media at InterTrust. "A robust electronic community of people exchanging content in a safe way, where rights holders get paid and consumers feel good about the experience." (New York Times 28 Jun 2000)

2000-07-11 **Keywords:** intellectual property IP licensing Web royalties lawsuit judgement

NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/ap/docs/185784l.htm>

#### Vol #

A federal judge . . . ruled that the Web site Gridiron.com violated the exclusive licensing rights of the National Football League's Player Association by using the names and images of NFL players without paying royalty fees. The site allows visitors to search for players by name, team and position. The executive director of the Player's Association said, "Gridiron.com's Web site was a direct attack on the rights and resources the union uses to protect players through collective bargaining." (AP/San Jose Mercury News 11 Jul 2000)



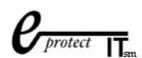


2000-07-12 **Keywords:** intellectual property IP fair use legislation law proposal NewsScan (reprinted with permission), Washington Post < http://www.washingtonpost.com/wp-dyn/articles/A24504-2000Jul11.html>

#### Vol #

Senate Judiciary Committee chairman Orrin Hatch . . . [said] that Congress may want to "tweak" the definition of "fair use" in intellectual property law because of the unwillingness of the recording industry to allow music fans to use the Internet to download and swap digital music files using Napster or similar new technology. In testimony before that committee, Napster's chief executive Hank Barry insisted: "Napster does not copy files. It does not provide the technology for copying files. Napster does not make MP3 files. It does not transfer files. Napster simply facilitates communication among people interested in music." But Lars Ulrich of the rock group Metallica told the committee: "Napster hijacked our music without asking. We should decide what happens to our music, not some company with no rights in our recordings. The choice has been taken away from us." (Washington Post 12 Jul 2000)





2000-07-21 **Keywords:** intellectual property IP peer-to-peer network music copyright violations infringements trading lawsuit

NewsScan (reprinted with permission)

#### Vol #

A coalition of trade groups representing more than 20 entertainment and film companies has sued Scour, a company backed by Hollywood powerbroker Michael Ovitz, which has developed a Napster-like search engine that enables users to trade films and music on the Web. The case is similar to the recording industry's lawsuit against Napster, whose service enables users to swap songs for free by trading MP3 files. Both suits seek preliminary injunctions to have unauthorized copyrighted material pulled off these sites, claiming losses in revenues and creative control for artists. Scour president Dan Rodrigues expressed surprise at the lawsuit, saying he was engaged in productive talks with Sony, Warner and Bertelsmann's BMG to establish business relationships with these companies. But Jack Valenti, president and CEO of the Motion Picture Association of America, one of the plaintiffs, said: "This is about stealing, plain and simple. Creative works are valuable property and taking them without permission is stealing, whether you download movies illegally or shoplift them from a store." (Financial Times 21 Jul 2000)

2000-07-25 **Keywords:** intellectual property IP culture history

NewsScan (reprinted with permission), Los Angeles Times < http://www.latimes.com/business/20000725/t000069563.html>

#### Vol #

Time Warner president Richard Parsons says the court's decision on Napster will have major effect on the future of society: "I think this is a very profound moment historically. This isn't just about a bunch of kids stealing music. It's about an assault on everything that constitutes the cultural expression of our society. If we fail to protect and preserve our intellectual property system, the culture will atrophy. And corporations won't be the only ones hurt. Artists will have no incentive to create. Worst-case scenario: The country will end up in a sort of cultural Dark Ages." (Los Angeles Times 25 Jul 2000)





2000-08-03 **Keywords:** intellectual property IP royalties shareware publishing NewsScan (reprinted with permission), CNet < http://news.cnet.com/news/0-1007-200-2419316.html>

#### Vol #

The new Stephen King novel, published on the Web with a request that at least 75% of downloaders send the author \$1 for the privilege, may well change the way all sorts of intellectual property is marketed, says R. Polk Wagner, a Penn law school professor. "Traditional intellectual property theory holds that producers (that is, King) won't produce unless they have the ability to restrict the access of others to their goods. Here King is doing two significant things: First, he's only asking 75 percent of the people to pay him, thereby engaging in an unusual form of price discrimination where only those who feel the moral pressure to contribute will do so. That is, King acknowledges that not everyone will pay. Second, he's explicitly asking people to pay for his future services. The traditional theory of intellectual property would not consider this possibility. Classic intellectual property theory holds that producers must get paid for the works they've already created, not works they've yet to produce." The result could be troubling for publishers, who depend on the sacredness of intellectual property for their livelihood. "If Stephen King, one of the 'poster boys' of the intellectual property industry, doesn't need intellectual property (protection) anymore, what does that mean for intellectual property generally?" (Knowledge@Wharton 3 Aug 2000)





2000-08-04 **Keywords:** intellectual property IP royalties Web publishing freelance writers NewsScan (reprinted with permission), Hollywood Reporter

< http://www.hollywoodreporter.com/archive/hollywood/current/webwatch/webwatch06.asp>

#### Vol #

The National Writers Union's executive board . . . reached an agreement with Contentville, an online reseller of text-based "content," that will give freelance writers a 30% cut of the fees paid by Contentville customers. Royalties would be distributed through the NWU's Publication Rights Clearinghouse. Contentville sells, for a small fee, "books, magazines, e-books, academic works, transcripts, archived articles, scripts or anything else that qualifies as brain food." The truce signals a new desire on the part of Internet publishers to settle the messy issue of electronic posting of written works that were created under agreements that did not expressly provide for e-publication. The issue has rankled the freelance community as many heavyhanded media companies have for the last few years required freelancers to sign contracts that allow electronic republication of their work without additional compensation. Last September, a U.S. federal appeals court ruled that publishers can't include work by freelance writers in their electronic databases without the writers' permission. Among the companies that had fought the federal case were The New York Times Co., Newsday, Time Inc. Magazine Co., University Microfilms International and Mead Data Central Corp. The Times and Time Inc. have said they will appeal the decision to the Supreme Court. (AP/Hollywood Reporter 4 Aug 2000)

2000-08-07 **Keywords:** intellectual property IP lawsuit infringement copyright

NewsScan (reprinted with permission), Los Angeles Times

< http://www.latimes.com/business/20000807/t000073815.html>

#### Vol #

The New York Times, Washington Post, and other traditional media companies are suing the San Diego company GoSMS.com for redistributing articles without their permission. GoSMS.com copies the articles from the original Web sites in order to ship them to the handheld devices of its own customers. (Los Angeles Times 7 Aug 2000)





2000-08-11 **Keywords:** intellectual property IP copyright infringement violation distribution NewsScan (reprinted with permission), Hollywood Reporter < http://www.hollywoodreporter.com/archive/hollywood/current/webwatch/webwatch05.asp>

Vol #

Bowing to pressure from the recording industry, America Online . . . removed a search engine used to find music files on its Winamp.com site, which distributes a popular MP3 player program for Windows. "We don't have an efficient process for distinguishing between legal and illegal MP3s, so we decided to take it down until we can address that," . . . [said] an AOL spokesman. The search engine was located on a site belonging to Nullsoft, an AOL subsidiary, whose staff describes themselves as "legitimate nihilistic media terrorists as history will no doubt canonize us." (AP/Hollywood Reporter 11 Aug 2000)

2000-08-17 **Keywords:** intellectual property IP body image ownership actor model avatar NewsScan (reprinted with permission)

#### Vol #

The sale of Press Association virtual newscaster Ananova to wireless operator Orange for \$143 million signals a new era for virtual reality, in which electronic virtual assistants, or EVAs, are poised to assume the roles of customer service representatives, celebrity spokespersons and shopping assistants. Digital Animations Group, the Scottish creators of Ananova and her successor, TMmy, is gearing up to market similar EVAs to online businesses that want to present a more "human" front. "It is our belief that virtual characters are going to dominate as personal assistants, presenters and even games celebrities," says Digital Animations CEO Mike Hambly. Meanwhile, U.K.-based Stratumsoft believes that EVAs based on real people have more potential. One possibility cited is supermodel Claudia Schiffer: "We could create a body scan of her, then produce an EVA based on her personality. As a marketing device, you would then have a celebrity available 24 hours a day on the Web site to 'chat' to fans and promote your product as part of your advertising campaign." What's not yet clear in all this is who would own such characters — the brand or the "real" celebrity? (Financial Times 17 Aug 2000)





2000-08-21 **Keywords:** peer-to-peer networking intellectual property IP

NewsScan (reprinted with permission), Hollywood Reporter < http://www.hollywoodreporter.com/music/index.asp?ee>

Vol #

Music industry officials say the only way to combat music piracy is to develop their own universal platform for selling music online. "We need an open system where all our music is available; we can't leave it to Napster or Gnutella," says Rudi Gassner, a board member for Germany's Edel Music. According to BMG Entertainment exec Thomas Stein, within five years, Internet sales will account for 50% of the music retail business, compared with 3.4% today. Meanwhile, Bertelsmann CEO Thomas Middelhoff says music companies need to digitize their back catalogues, secure the legal rights to sell their music online, and synchronize their technical standards. "We have to sit down -- without the entertainment lawyers -- and come to an agreement." (Hollywood Reporter 21 Aug 2000)

2000-09-05 **Keywords:** intellectual property IP licensing copyright royalties government proposal law regulation tax

NewsScan (reprinted with permission)

Vol #

The German government is considering levying a fee on manufacturers of computer and telecommunications equipment that can be used to duplicate protected works. The fee would be used to compensate authors and other copyright holders. Included under the amendment would be such devices as CD burners, computer printers, hard drives and high-speed modems that facilitate large file downloads. Such fees are already levied on copy machines. Industry officials have denounced the plan, which they say would raise the price of such devices by 30% in Germany. A Hewlett-Packard executive told the Berliner Zeitung that many companies would simply move their operations out of Germany if the tax is passed. (AP/San Jose Mercury News 5 Sep 2000)





2000-10-27 **Keywords:** copyright intellectual property ruling limitations libraries filtering censorship censorware

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB972602565773912484.htm >

#### Vol #

In a step toward revamping traditional copyright law to reflect the realities of the digital age, the federal Copyright Office has issued a ruling backing companies' rights to limit access to their content when it is made available on the Internet. The decision came as part of new federal law that makes it illegal for Web users to hack through software that copyright holders use to protect books, films, music and other digital content. Congress had left it to the Copyright Office to create any exemptions that might be needed to facilitate access by libraries and universities. The two exemptions allowed are minor in scope: one enables users of filtering software to access the lists of Web sites being filtered, and the other gives people the right to bypass malfunctioning security features of software and other copyrighted goods they have purchased. The decision came as a blow to libraries and universities because it gives copyright holders a whole new level of protection, which they fear could limit their ability to use materials in digital format. An American Library Association official said the decision will "significantly impede efforts for libraries to continue to provide information in the digital age." (Wall Street Journal 27 Oct 2000)



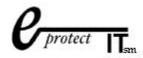


2000-11-27 **Keywords:** intellectual property government regulation fee tax copyright NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB975279995969460074.htm >

#### Vol #

Hewlett Packard became the first company to be snagged by a German law that requires CD burner manufacturers to pay a fee for each device sold in that country. HP reached an agreement last week with GEMA, Germany's main licensing group, to pay DM3.60 (US\$1.54) for each CD burner sold since February 1998, when the issue first arose, and DM12 (US\$5.16) for each CD burner sold in the future. The fees are distributed by GEMA to copyright owners through recording houses and music distributors. The development is being watched closely by many of Germany's neighbor's, including France, Italy and Greece, which have similar laws levying fees on makers of equipment that can be used to violate copyright laws. (Wall Street Journal 27 Nov 2000)





2000-12-11 **Keywords:** intellectual property copyright fees music government regulations broadcasting Webcasting

NewsScan (reprinted with permission), Hollywood Reporter < http://www.hollywoodreporter.com/music/index.asp?ee >

#### Vol #

[In late November, the] U.S. Copyright Office. . . [began] considering whether radio stations must pay record companies when the stations use their Web sites to offer music over the Internet. The radio industry . . . [was] not happy about the possibility. Dennis Wharton of the National Association of Broadcasters said: "What the music industry is trying to do is saddle broadcasters with new fees that Congress has always exempted us from paying. It could cost broadcasters millions of dollars and would probably cripple or seriously impair the streaming of radio signals over the Internet." (Bloomberg/New York Times 27 Nov 2000)

[In early December, the] recording industry won a victory . . . when the U.S. Copyright Office ruled that Webcasting by radio broadcasters constitutes a second performance of artists' copyrighted works and does not merit the same exemption from royalty payments accorded to traditional over-the-air programming. "Transmissions of a broadcast signal over a digital communications network such as the Internet are not exempt from copyright liability," the Copyright Office wrote. Broadcasters had argued that their Webcasts were exempt because they are "nonsubscription" transmissions licensed by the FCC that serve local communities, but the Copyright Office rejected that argument, pointing out that, in fact, Webcasts exceed "the geographic limits established for broadcast under the FCC license." The decision could mean millions of dollars in royalty fees that companies like Bertelsmann, Universal and Warner Bros. would collect from broadcasters. (Hollywood Reporter 11 Dec 2000)





# 4B2 Patents

2000-02-28 **Keywords:** personalization intellectual property privacy

NewsScan (reprinted with permission), Salon.com < http://www.salon.com/tech/feature/2000/02/28/geographic/index.html>

#### Vol #

iCraveTV founder Bill Craig says he's developing technology that will indicate a Web surfer's geographic location when he or she logs on to a site, enabling the site operator to send pages targeted to people in that region. "It would be a huge breakthrough for the Internet and for copyright holders," says Craig, who would also stand to benefit, because it would enable him to sidestep the current controversy over his business of streaming video of sports events and movies to which he doesn't own the rights. The service is legal in Canada, but has unleashed protests from broadcasters in the U.S., and in January a U.S. judge ordered iCraveTV to stop the streaming. Craig is hoping that his "geographic intelligence" technology will alleviate concerns over iCraveTV, and maybe grow into an even more lucrative business than streaming TV broadcasts. "We want to build a business where we can go to rights holders and say, 'You want it released only in Canada, you've got it; in the U.S., you've got it,'" says Craig. (Salon.com 28 Feb 2000)





2000-03-10 **Keywords:** software patents

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cth529.htm>

#### Vol #

Amazon CEO Jeff Bezos says that even though his company has received two potentially profitable e-commerce technology patents, he believes the length of time that patents protect a piece of software code is too long. "Especially in the age of the Internet, a good software innovation can catch a lot of wind in three or five years," Bezos wrote in an open letter to customers and Internet users (http://www.amazon.com/exec/obidos/subst/misc/patents.html/102-6583935-10424 35). He proposes drastically shortening the current 17-year term, and instituting a one-month public comment period prior to issuing patents so that other companies with similar or superior technology could ensure their rights are protected. Bezos says his company will retain its 1-Click and Amazon Affiliate patents, but will enforce them only "when there are important business reasons for doing so." (AP/USA Today 10 Mar 2000)

2000-03-29 **Keywords:** patent regulations law research revamp change alter improve

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB954286078412266261.htm>

#### Vol #

The U.S. Patent and Trademark Office is overhauling the way it reviews applications for many online practices, and will now require a broader search of past practices and inventions before awarding patents. The change comes in response to critics who charge the Office with granting overly broad patents for basic Web techniques, such as Amazon's "1-Click" ordering process. Examiners reviewing applications in the business-method area will now have to follow new procedures, including searching online databases for similar technology ideas. "If you make these decisions without adequate data, you run the very real risk of issuing patents on things that were already invented, or patents that are far broader than they should be," says Roland Cole, executive director of the Software Patent Institute. (Wall Street Journal 29 Mar 2000)





2000-06-01 **Keywords:** intellectual property lawsuit patent infringement privacy exhibitionism NewsScan (reprinted with permission), New York Times < http://www.nytimes.com/library/tech/00/06/biztech/articles/01voyeur-lawsuit.html>

### Vol #

Entertainment Network Inc., which operates a Florida-based Web site that paid college tuition for a half dozen women who agreed to have cameras situated throughout their group house sending 24-hour-a-day live video feeds of all aspects of their daily lives, . . . [sued] CBS and Infinity Broadcasting for allegedly stealing the site's marketing strategies and technical expertise. CBS and Infinity, who . . . [were] developing a similar program called "Big Brother," . . . [said] the suit . . . [was] frivolous. (AP/New York Times 1 June 2000)

2000-06-02 **Keywords:** intellectual property advertising Web lawsuit patent infringement NewsScan (reprinted with permission)

### Vol #

Juno Online Services . . . [sued] NetZero and Qualcomm for alleged patent infringement. Juno . . . [said] that the two companies . . . unlawfully made use of a technology developed by Juno that downloads advertisements and other content and displays it on a user's PC following an online session. (Bloomberg/Los Angeles Times 2 Jun 2000)





2000-09-13 **Keywords:** intellectual property IP software copyright patent international agreement NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB968792884357682385.htm>

### Vol #

An administrative board for the European Patents Office has voted 10-9 to allow patents for software in Europe, with a final decision coming in November at a conference of the all the countries represented by the Office. Software patents are available in the U.S. and Japan, and multinational companies have been arguing for unlimited patenting as part of a uniform global legal framework. Critics, however, fear that large companies will use the patenting process as a tool to squelch innovative technologies that threaten their standard products. Among the dissenting countries were Germany, the U.K. and France. The head of the German delegation expressed his reservations over the change: "We would have problems with the U.S. tendency to patent everything that can be patented. That would stifle innovation and cause a glut of litigation." (Wall Street Journal 13 Sep 2000)





2000-09-30 **Keywords:** intellectual property patent hyperlink litigation royalties court lawsuit NewsScan (reprinted with permission), New Scientist < http://www.newscientist.com/news/news.jsp?id=ns225851>

### Vol #

It turns out that British Telecom has owned a U.S. patent covering hyperlinks for the last 14 years, but up until . . . [June had] made no attempt to exploit the patent commercially. The patent, which expires in 2006, was buried among 15,000 other global patents owned by the telecom giant until it was rediscovered "a few years ago" during a routine review of the company's intellectual property. BT has now decided to commercialize the technology, which allows Web surfers to move between pages by clicking on pictures or text — a move that could earn BT hundreds of millions of pounds. "We are not trying to stop anybody using the Internet. We simply want some reasonable royalties based on the revenues that other organizations are enjoying from making use of this intellectual property," BT said in a statement Monday. "We are not trying to take anything away from Tim Berners-Lee, but [BT] did invent a way of structuring information to make it easily accessible." The company added that it has spent the last two years researching its claim to the technology to make sure it holds up in court. "It is not something you want to shoot from the hip on," it said. (Financial Times 20 Jun 2000)

[However,] British Telecom's claim that it patented Internet hyperlinking technology back in 1976 . . . hit a snag [in September]. The U.S.-based Internet Patent News Service . . . [pointed] patent lawyers to a Web site (http://sloan.stanford.edu/MouseSite/1968Demo.html) that hosts a 90-minute film shot by Stanford University in 1968 featuring Douglas Englebart demonstrating the first computer mouse -- and using it to click on hyperlinks. (New Scientist 30 Sep 2000)





2000-10-04 **Keywords:** patent business method legislation

NewsScan (reprinted with permission), Computer User< http://www.computeruser.com/news/00/10/04/news5.html >

### Vol #

A new bill introduced by Reps. Rick Boucher (D-Va.) and Howard Berman (D-Calif.) seeks to strengthen the review process for companies wishing to patent a "business method." The U.S. Patent and Trademark Office has recently come under fire for issuing patents to Amazon.com for its "1-click" check-out model, and to Priceline.com for its "name your own price" e-commerce service. These overly broad patents have led to unnecessary lawsuits over common business practices, say critics. "Something is fundamentally wrong with a system that allows individuals to get patents for doing the seemingly obvious," said Boucher. The Business Method Patent Improvement Act would require the Patent Office to publish all business method patent applications after 18 months, and would offer an administrative "opposition" process to settle disputes without litigation. It would also discourage patents on processes whose only distinguishing factor is that they use a computer to accomplish the task. (Computer User 4 Oct 2000)

2000-12-28 **Keywords:** patent infringement lawsuit

NewsScan (reprinted with permission), Hollywood Reporter < http://www.hollywoodreporter.com/convergence/index.asp?ee >

### Vol #

NetZero, a free Internet access provider, has filed a patent infringement lawsuit against rival Juno Online Services. The suit alleges that NetZero's patent covers the technology used to present an on-screen advertising window that pops up separately from an Internet browser. Juno has responded that "On the contrary, we believe that NetZero has been infringing on a key patent held by Juno, in connection with which Juno filed a lawsuit against NetZero in June of this year." (Hollywood Reporter 28 Dec 2000)





# 4B3 Reverse engineering





2000-03-16 **Keywords:** Internet content filtering censorware reverse engineering hacking civil lawsuit restraining order

AP, NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cth570.htm> ; RISKS

Vol 20 # 85

Microsystems Software Inc. (Framingham, MA) filed a civil lawsuit in mid March 2000 against two software experts who reverse engineered their Cyber Patrol software. Eddy L. O. Jansson (thought to live in Sweden) and Matthew Skala (a graduate student in computer science at University of Victoria in British Columbia, Canada) posted a utility called "cphack" on the Web to allow kids to determine their parents' password for the program's administration functions and thus bypass Cyber Patrol filters. The software was instantly posted around the world, making it impossible to stop the spread of the anti-censorware regardless of what the authors do.

Bear Giles, a frequent and always lucid commentator in RISKS, wrote that the entire question of encrypting the blacklists should be examined. Are these lists of forbidden sites concealed to protect children? Against what? "[H]ow would knowing that a site is on the blacklist permit a kid to access the blocked site? How many kids have the technical knowledge to edit the blacklist?" Giles asked whether such lists are encrypted as an anticompetitive measure and to prevent users and analysts from determining the rate of false positives (exclusion of sites on spurious grounds).

A federal judge in Boston . . . [ordered] a halt to distribution of the "cphack" software created by two computer hackers by reverse-engineering the commercially distributed "Cyber Patrol" program that allows parents to shield their children from pornography on the Internet. The judge's order also applies to any mirror Web sites where the program has been made available. Peter Junger, a law professor and free speech advocate, calls the ruling "a rather horrifying challenge to people's right to write software" and to figure out how it works by taking it apart and examining it. (USA Today 17 Mar 2000)





2000-03-24 **Keywords:** Internet content filtering censorware reverse engineering hacking civil

lawsuit restraining order subpoena court documents e-mail forgery

delivery reliability

NewsScan (reprinted with permission)

Vol #

In the MicroSystems case against two hackers who reverse-engineered that company's "Cyber Patrol" filtering software in order to create a "cphack" program to thwart its effectiveness, MicroSystems attorney Irvin B. Schwartz prevailed on U.S. District Judge Edward Harrington to allow him to send e-mail copies of the restraining order to anyone who is distributing a copy of cphack. Schwartz says, "It makes sense. You want to put people who might conceivably be in violation of a court order that they're on notice... It provides a medium to serve the court's order at Internet speed as opposed to snail mail or even worse, by courier." But Wired magazine columnist Declan McCullagh charges that the e-mails are "subpoena spam" and says: "E-mail is easy to forge. I can't even be certain it really did come from a real lawyer." (AP/San Jose Mercury News 24 Mar 2000)

http://www.sjmercury.com/svtech/news/breaking/merc/docs/079231.htm





2000-03-28 **Keywords:** Internet content filtering censorware reverse engineering hacking civil lawsuit restraining order copyright

POLITECH, Wired

Vol #

The Mattel suit trying to stop distribution of cphack moved to the next stage on March 28, 200 when Judge Edward Harrington of the US District Court in Boston ruled that all mirror sites must remove copies of cphack or face legal consequences. In an interesting twist, Mattel declared in court that it now owned the copyright for cphack and therefore could control its distribution. However, Declan McCullagh pointed out that the original software was released under the GNU General Public License, apparently permitting anyone to distribute the code for free regardless of later copyright claims.

In early April, the ACLU filed suit for a stay of Judge Harrington's order while they appealed his ruling.





2000-04-15 **Keywords:** legislation software license back door denial of service DoS

Crypto-gram < http://www.counterpane.com/crypto-gram-0004.html >

**Vol** 00 # 04

Bruce Schneier of Counterpane Internet Security <

http://www.counterpane.com/index.html> analyzed the disastrous Uniform Computer Information Transactions Act (UCITA) which was signed into law in Virginia and Maryland. Specifically, he pointed out that the Act allows software makers to include a back door so they can remotely disable software if users fail to abide by the terms of their license. As Schneier wrote, "The naive conceit here is that only the manufacturer will ever know this disable code, and that hackers will never figure the codes out and post them on the Internet. This is, of course, ridiculous. Such tools will be written and will be disseminated. Once these tools are, it will be easy for malicious hackers to disable peoples' computers, just for fun. This kind of hacking will make Back Orifice look mild." As for using public-key cryptography to ensure that only authorized instructions could be effective, Schneier commented that such assurances would depend upon perfect implementation of cryptography; however, "Given the industry's track record at implementing cryptography, I don't have high hopes."





2000-10-20 **Keywords:** intellectual property lawsuit ruling copy protection fair use reverse engineering Digital Millennium Act copyright

NewsScan (reprinted with permission)

### Vol #

With a decision that represents a defeat for universities, libraries, and computer programmers but pleases media companies such as Sony and Time Warner, the U.S. Copyright Office . . . endorsed a provision of a new federal law making it illegal to use "reverse engineering" to learn how to evade the technological safeguards protecting copyrighted material. The provision in question is part of the 1998 Digital Millennium Act, and Congress had asked the Copyright Office to review it before it took effect. Academic and research institutions had argued that the restriction against reverse engineering was counter to the spirit of the "fair use" principle that allows limited kinds of free use to copyrighted materials under certain, specified conditions. (New York Times 30 Oct 2000)

http://www.nytimes.com/2000/10/30/technology/30LIBE.html

2000-11-26 **Keywords:** regulation software reverse engineering contract law

 $Computer\ Professionals\ for\ Social\ Responsibility < \ http://www.cpsr.org/program/UCITA/ucita-fact.html >$ 

### Vol #

The Computer Professionals for Social Responsibility (CPSR) published a fact sheet about the Uniform Computer Information Transactions Act (UCITA) < http://www.cpsr.org/program/UCITA/ucita-fact.html > . Among other resources, the fact sheet includes a useful link that keeps track of developments in state legislatures. Another useful resource is the July 1999 essay by Cem Kaner and David Pels at < http://www.badsoftware.com/kaneropd.htm > .





# 4C1 Paradigms

2000-05-11 **Keywords:** software quality assurance QA liability pressure

NewsScan (reprinted with permission)

Vol #

In testimony provided to the Congressional subcommittee holding hearings on the love bug virus, noted computer security expert Peter G. Neumann of SRI International warned that the software industry is not doing what it should to keep the Internet safe: "Vastly many more people are now relying on the Internet, and most of them are oblivious to the risks... Overall, the situation is grave. The commercial marketplace is not leading. The government is not exerting enough driving forces. This is a really ridiculous predicament, and would be a very bad joke if it were not so serious... Until software developers and system purveyors are liable for the failures of their products, there will be no real motivation to develop robust systems... The mass-marketplace is overly concerned with features; it tends to be long on fancy features and to ignore critical requirements such as rudimentary robustness. However, robust features can be achieved with good design and good programming practice, rather than the business-as-usual practices of sloppy development and a rush-to-market mentality. If automobiles were recalled as often as computer system flaws are detected, we would still have horses and buggies." (New York Times 11 May 2000)





2000-07-17 **Keywords:** web of trust confidence paradigm system ratings vulnerabilities

NewsScan (reprinted with permission), Wall Street Journal < http://interactive.wsj.com/articles/SB963786024674216913.htm>

Vol #

With cyberfraud proliferating at Internet speed, the question of trust on the Internet is prompting some netizens to develop new systems known as "reputation managers" that attempt to "computerize" a trust function for wary Web surfers. One of the most sophisticated examples is Epinions.com, which solicits and compiles people's reviews of a variety of products and services. As you read the writeups, you tell Epinions which were most "trustworthy" and helpful, and the next time you return, Epinions prioritizes them based on who has earned your trust. The Google search engine works on a similar system, with each Web page in its database ranked by how many other sites link to it. Each link is counted as a "vote" for the trustworthiness of that site. In contrast, eBay's feedback system, in which every buyer who successfully completes a transaction gets to rate the seller, is fraught with potential for fraud. Jakob Nielsen, a Web design specialist who studies reputation systems, says "The eBay system actually works perfectly if everyone is completely honest. But if you can put in your own rating, it falls apart." (Wall Street Journal 17 2000)

2000-09-25 **Keywords:** policy punishment unexpected consequences zeal overreaction incident response

RISKS, Christian Science Monitor < http://www.christiansciencemonitor.com/durable/2000/09/26/fp2s2-csm.shtml >

Vol 21 # 07

In the wake of the prosecution of Wen Ho Lee, staff at the Los Alamos National Laboratory of the U.S. Department of Energy became wary of reporting any security violations. This is an example of the law of unintended consequences and illustrates the foolishness of using punishment as the sole mechanism for encouraging secure behavior.





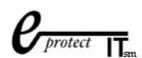
2000-12-06 **Keywords:** conference paradigm social relations trust community

NewsScan (reprinted with permission) < http://www.code.uni-wuppertal.de/uk/trust/welcome.html >

### Vol #

Dr. Mihai Nadin, professor of computational design at the University of Wuppertal in Germany says, "Our age is characterized by shorter cycles of innovation, faster processes, decentralization, and discontinuity. Permanence is at best a nostalgic desideratum connected to a past that for certain intervals had an appearance of stability. Our time is one of instability, higher speeds, and a human scale of pragmatic activity that has reached globality. Behind these loaded words is the simple realization, by each and every one of us, of a state of flux. After all is said and done: Is trust still possible today?" To answer that question, the University of Wuppertal will convene an international colloquium on "TRUST" on 16-17 January 2001.





2000-12-12 **Keywords:** security alerts publication details Web link URL controversy discussion debate completeness

**RISKS** 

**Vol** 21 # 16

Chris Adams summarized a debate over new, more limited forms of bug alerts. Some companies, including Microsoft, are publishing their alerts with much less technical information and referring interested readers to their Web site for full details. Adams criticized this practice, arguing that (quoting him verbatim):

- \* Access for people with marginal Internet connections or browsers other than IE/Netscape is less convenient.
- \* Information is unavailable if the Web server is down or overloaded, as might happen with an important advisory. It seems counterproductive to put important, time-sensitive material behind a single point of failure, particularly when the decision is to deliberately avoid using a free distributed, fault-tolerant distribution channel.
- \* It makes it much easier for a vendor to change an advisory without notifying anyone, especially since changed or removed advisories won't be archived in anywhere near as many places as a mailing list such as BUGTRAQ. In addition to covering up bad work, this would also make it easier to remove or tone-down past advisories about companies the author is now aligned with.
- \* It opens the prospect of tailoring content to the reader. This could be as simple (and annoying) as charging for access to some content or as complex as determining what to show based on where the request came from (e.g. competitors, vendors or journalists). While this would probably be caught for something major, particularly at first, it would not surprise me to find at least subtle tampering happening regularly if this becomes commonplace.

In a follow-up posting, a report by Richard M. Smith on BUGTRAQ stated that the new Microsoft security bulletins include Web bugs, presumably to track how many people read the bulletins.





# 4C2 Risk management

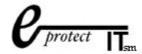
2000-01-17 **Keywords:** cybercrime insurance risk management

National Underwriter Property and Casualty

Vol #

Several insurance companies began providing insurance to pay for damages resulting from illegal penetration of computer systems and networks and even against extortion. For example, in May 1999, the F&D/Zurich company in Baltimore announced policies with up to \$25M in compensation for damages to e-businesses. Some policies cover insider damage such as logic bombs or destruction of critical data by enraged employees; Brad Gow of ACE USA in Philadelphia reported on one case where an employee at a Massachusetts defense contractor "destroyed all their critical databases and project data. The company identified direct costs of rebuilding data at about \$2.4 million." Daniel Hays, writing for the \_National Underwriter Property and Casualty\_ publication, said that estimated total loss from missed sales and other opportunities and other setbacks to that business were projected to be \$10 million.





2000-04-02 **Keywords:** Internet security monitoring log files audit trails intrusion-detection NewsScan (reprinted with permission), San Jose Mercury News < http://www.sjmercury.com/svtech/news/breaking/merc/docs/006917.htm>

Vol #

A new Internet security company called Counterpane Internet Security Inc., organized by well-known author and consultant Bruce Schneier, will use teams of analysts continuously scrutinizing activity logs from customer Internet sites and sound the alert when there are signs of an intrusion. Schneier says, "Computer security without monitoring is kind of like having a car alarm go off in the inner city. It might make a lot of noise, but everyone ignores it." An executive of Computer Associates, the current industry leader in computer security, insists his company will continue following a different approach: "We have seen in this industry that throwing more people at a problem actually doesn't solve it. Our approach is to apply technology solutions to solve problems rather than throwing more warm bodies at them." (AP/San Jose Mercury News 2 Apr 2000)

2000-06-08 **Keywords:** backup failure e-mail loss destruction documentation RISKS

Vol 20 # 91

In April 1998, the Office of the Vice President migrated the e-mail server to Windows NT 4 and moved the e-mail files to a new partition which was not added to the backup schedule. In May 1999, staffers discovered that there were therefore no backups at all of any of the e-mail for the office over more than a year. [MORAL: documentation and proper procedures really DO matter.]





2000-06-14 **Keywords:** government operations outsourcing quality assurance QA

NewsScan (reprinted with permission), TechWeb < http://www.techweb.com/wire/story/TWB20000613S0012>

### Vol #

Prompted by results from its 15-month Project Groundbreaker feasibility study, the National Security Agency plans to use private sector sources to develop and maintain the bulk of its unclassified information technology infrastructure. This dramatic change in NSA's long-standing IT operations is intended to ensure the agency's agility and adaptability in the Information Age. The move to abandon the traditional policy of developing spy technology in-house in favor of procurement from the rapidly expanding encryption and fiber-optic technology available off-the-shelf was inspired in part by last January's massive computer failure that crippled NSA's global spy network for several days. The IT modernization will cover NSA's distributed computing, its enterprise/security management, networks and telephony. It is expected to save the government as much as \$1 billion over 10 years. (TechWeb 14 Jun 2000)

2000-07-10 **Keywords:** criminal hacker attack insurance penetration vandalism outsourcing monitoring intrusion detection

NewsScan (reprinted with permission), USA Today < http://www.usatoday.com/life/cyber/tech/cti199.htm>

## Vol #

Lloyds of London and two other insurance companies will offer up to \$100 million in insurance coverage to the clients of the computer security management firm Counterpane Security against losses resulting from attacks by network vandals. A Counterpane executive says, "This is not for your home user, this is for Yahoo!, this is for CDUniverse... It's threat-avoidance. This, along with monitoring, is just another arrow in your quiver." A recent study by Reality Research has predicted that businesses worldwide will lose an estimated \$1.5 trillion this year due just to computer viruses spread through the Internet. (USA Today 10 Jul 2000)





# 4D Funny / miscellaneous

2000-01-06 **Keywords:** criminal hackers gray-hat commercial company consulting AP,. New York Times, NewsScan, OTC, PC Week, TechnologyEvaluation.com

Vol #

Eight self-described top computer hackers who were members of L0pht Heavy Industries formed a new consulting firm called @Stake in January 2000. These people insisted that they would continue to use their hacker handles (e.g., Mudge, Weld Pond, Space Rogue, Brian Oblivion, Dildog) and claimed that they did not break into systems illegally. They were described in glowing terms by such security luminaries as Counterpane's Bruce Schneier ("They're very, very good -- first rate. . . .") and by NTBugtraq's Russ Cooper ("The eight brilliant geniuses down at the L0pht. . . ."). However, other commentators such as John Taschek of PC Week expressed horror at the move: "This is clearly an example of the farmer giving the fox the key to the chicken coop. I can't imagine that any legitimate startup would actually seek out L0pht." He added, ". . . L0pht's history shows that the group is not ethical, maintained practices that bordered on being illegal and is simply downright scary. I wouldn't want any organization that hired the brain trust of L0pht as my security consultant."

2000-01-13 **Keywords:** mouse ergonomics carpal tunnel syndrome

Edupage, New York Times

Vol #

According to research by Cornell University's Prof. Alan Hedge, there may be an advantage to using a larger computer mouse. Tests suggested that the larger devices might reduce strain on fingers and wrists. The author explicitly refused to claim that changing mouses would reduce carpal tunnel syndrome but suggested it might help.





2000-05-22 **Keywords:** generational experience QA quality assurance

**RISKS** 

**Vol** 20 # 89

Zygo Blaxell wrote about an alarming tendency among those who have grown up with bad software:

> While at a bookstore the other day, my spouse was presented with a credit card signature slip printed by an Interac point-of-sale terminal. It was just like any other credit signature slip, except that the usual "customer signature" line was printed twice, one on top of the other, with ample space for the signature in both places--a harmless glitch, probably due to an obvious and simple programming error.

We pointed the error out to the cashier, who was probably barely old enough to be legally employed, and her response, if she speaks for her generation, was ominous, even terrifying:

"It does that because ... because it's a computer."

An entire generation is growing up believing that the current sorry state of affairs in information technology could ever be accepted as \_normal\_!<





2000-07-12 **Keywords:** spoof joke humor

NewsScan (reprinted with permission), CNet < http://news.cnet.com/news/0-1003-200-2249491.html>

#### Vol #

A humorous posting on Bugtraq, a popular computer security e-mail list, . . . [warned] that hackers have found a way to take over Sony's Aibo robot dog and command it to attack and perform other annoying canine tricks. The posting, written in the style of security alerts issued by the Computer Emergency Response Team (CERT), warns: "The buffer used to hold the variable MyOwner in the function process\_face() can be overflowed, reverting Aibo into experimental AiboPitBull code." Other malicious codes that can affect Aibo's usually friendly and obedient nature include PeeOnRug(), ShoeChew() and KillTheCat(). In addition, "owners who accidentally have left their television on late at night have reported incidents of Aibo attacking their small children and pets within minutes of the airing of 'Tom Vu's Real Estate Seminar.'" CERT spokesman Shawn Hernan noted, "This is, of course, a forgery, but nonetheless pretty amusing." (CNet News.com 12 Jul 2000)

2000-07-14 **Keywords:** joke funny spoof amusing satire

RISKS, segfault.org < http://segfault.org/story.phtml?id=396f3e5c-0958dfa0 >

## **Vol** 21 #

Leonard Richardson posted an amusing spoof of the usual responses to new breaches of cryptographic algorithms, availability of cracker tools, and so on. The satirical piece began, "The well-known polynomial  $x^2 + 8x + 6$  was defaced today by a teenager who had "r00ted" the beloved function of one variable through the use of a popular script known as "QuAd 3QaZh0n". The attack set off the usual sequence of events: an initial panic setting off an orgy of media hype reaching a crescendo with an article in the mainstream media, a string of copycat successors, and a meaningless stream of empty promises from vendors who immediately lapsed back into apathy as the incident left the public's short-term memory."



