Organization for Security and Co-operation in Europe
The Representative on Freedom of the Media
Freimut Duve

Karin Spaink and Christiane Hardy

Freedom of the Internet – Our New Challenge

The Internet is a medium unlike any other. While it embodies aspects of different more old-fashioned media, it not only combines them but also adds features, inherent to its digital nature.

E-mail for instance can be compared with postal mail, but has the capacity to send carbon copies of letters to many people at once with the added bonuses of (almost) instantaneous delivery and of mail programs automatically archiving all correspondence, meaning that on top of this it is searchable. Internet Relay Chats (IRC), I Seek You (ICQ) and other protocols for *chat boxes* on the other hand are more comparable to telephones: they allow a real-time conversation with a person or a group and can log that conversation for private perusal.

Usenet – the collective newsgroups – resembles a huge public bulletin board, subdivided by subject, where people can post messages which are accessible to everyone, but it is also archived, meaning that the discussions are stored for future reference.

The *World Wide Web* (WWW) is best compared to the printed press and the broadcasting media. One person or group is usually responsible for the published content. But unlike the traditional media, websites are accessible from all over the world, can be browsed by anybody on the planet, and they are usually free. Publishing on the Web is not only quicker and cheaper than via traditional printing and broadcasting but can also at any level combine texts with moving images and sound. And while some subjects never get covered by the traditional media – because the designated audience is too small or the material is too vast to be incorporated in an article or a book – the Net offers plenty of (cheap) space and website owners often excel in providing niche information. The information on this myriad of websites is divulged via search engines which, through the creation of huge indices, guarantee that everything is retrievable and accessible. The most localized, obscure or specific information is suddenly available to everyone, everywhere.

These shared and new characteristics have brought all known problems pertaining to old technologies into the Net, and a few new ones, too. Government censorship and the classic inaccessibility of information to the poorest masses are there, but now we have also the novelty of censorship performed by companies and of violation of privacy by governments on a scale that was previously unheard of and would have been impossible – if only for practical reasons – in the classical communication media.

Filtering as a Means of Censorship

A measure that many censor-minded countries deploy is the use of restrictive proxies. A proxy is basically a web server at the Internet Service Provider (ISP) level that fetches all pages requested by the users for them. By keeping local copies of pages that are visited frequently, the proxy is able to serve them faster and with less long-distance traffic. But proxies can also be used to *block* user requests for sites, based on an automatic check on their name, location and/or content. These restrictive proxies prevent Internet users from visiting forbidden sites and, in some instances, are even equipped with a tool that warns the police that someone has tried to access banned material. Singapore uses nationwide proxies in order to prevent access to certain websites, mostly those discussing religion or politics or depicting sex. (1) This government-imposed ban is not completely efficient: with some technical knowledge, the mandatory proxy can be circumvented. (2)

Dubai on the other hand uses a very strict proxy, imposed upon the country at the beginning of 1997. Whenever a net user attempts to visit a site that the Government has ruled out, the following message appears on the screen: "Emirates Internet Control List: access to this site is denied." (3) This nationwide proxy disallows Dubai citizens from visiting most newsgroups and blocks "selected sites on the Internet which negate local moral values". (4) The only sure way to circumvent such a proxy, is by dialing-up a provider in a different country, which often is not a viable recourse.

Basically, via such a proxy all international traffic can be monitored, thwarted and/or registered. To some degree, the practice is similar to a government blocking the reception of BBC world. But a restrictive proxy is much more effective and encompassing: in comparison to analogue communications, you could say that apart from blocking foreign radio stations, it also controls all import of books, all postal mail and all foreign press simultaneously.

It is not only dubious democracies that place restraints on the use of the Net. Australia does the same, although to a much lesser degree. Citizens can report pages that they deem to contain "explicit nudity" or to be in "poor taste" to a government authority, which then investigates the page and can order all national ISPs to block access to that particular page via their proxies. Electronic Frontier Australia (EFA), a group that protects and promotes on-line civil liberties, has complained about the poor accountability of the said government authority regarding the handling of such complaints. (5) The United States of America have previously tried to do something similar via their 1995 Communications Decency Act, which prohibited the publishing of "obscene, lewd, lascivious, filthy, or indecent" material on the Internet. Fortunately, in 1997 the Supreme Court ruled the CDA to be unconstitutional. (6)

Germany has twice tried to block specific material from their citizens as well. In 1995, the magazine *Radikal* was put online in the Netherlands after it was banned in Germany. (7) In 1996 and 1997, the German Government forced German providers to block *all* pages hosted by that particular Dutch ISP, XS4ALL, thereby making thousands and thousands of undisputed pages of XS4ALL's other users inaccessible as well. Because mirrors of the disputed pages sprang up everywhere, the blockade turned out to be futile and was cancelled after a month in both instances.

New attempts at filtering information keep being made. In the USA, publicly funded schools and libraries were at one point obliged to use rating and filtering systems that block web pages based on sexual content and/or graphic depictions of violence. Many people argued that these filtering systems curtail free speech and block many more pages than they promise to, (8) and a Virginia library taking precisely that stance successfully fought the Child Online Protection Act (COPA) in court. (9) However, recently a new bill was passed in the USA, again imposing mandatory filtering on schools and libraries that receive public funds. (10) This bill is currently being fought too, this time by the ACLU, the American Civil Liberties Union. (11) Undoubtedly, if the ACLU wins, the US Congress will come up with yet another filtering bill.

Since most Eastern European governments are not yet very familiar with the Internet – and since curtailing societies tend to be more aware of and monitor middle-tech communication more effectively than either the high-tech or the low-tech variants, there have been some instances of the Internet being used as an excellent device to circumvent government censorship. A famous example is B92, the independent Belgrade radio station that was forced off the air in 1999. The Dutch ISP XS4ALL used a direct cable connection between Belgrade and Amsterdam, inviting people in Belgrade to upload their audio files over the Internet and broadcasting them from Amsterdam over the Net in a real-time format that could be listened to or stored. In turn, many Serbs – especially those working at universities and international companies – captured and copied what they heard over the Net and distributed these radio programmes via audio cassettes, thus spreading the high-tech Internet broadcasts via low-tech means. There wasn't much that the Milosevic Government could do: while B92 broadcasted from the Netherlands, B92 could not be stopped at the source and Yugoslavia lacked the infrastructure to impose proxies upon its citizens.

Whose Constitution, Whose Jurisdiction?

Looking at laws being passed and jurisprudence and practice developing in Western European countries, one can attempt to foresee the future of freedom on the Internet. At this moment the future doesn't look too bright. While once the Internet was regarded as a way to route around censorship, by now, censoring and monitoring authorities are using the Net to route around national borders.

For one, we have Echelon: the joint USA/Canada/UK/Australia/New Zealand venture that monitors all digital communications passing the Atlantic, be it via fax, telephone or e-mail. The countries involved have long denied the existence of Echelon, but by now the European Parliament has investigated the rumours and has established its existence. Interestingly, the main complaint of the European Parliament is that the US, through Echelon, could be engaging in industrial espionage and thus gaining an economic advantage over European companies. The European Parliament hardly complained about the monitoring of European citizens as such. (12) And what is the use of having a constitution safeguarding your right to private communications when *another* government is preying on them? Then there is Carnivore: a US based system that intercepts e-mail and checks it automatically for words and terms deemed to be related to terrorism. Nobody knows the scope of Carnivore interceptions, nor is the list of "dangerous" terms public. The only thing known about

Carnivore is its unprecedented and massive capacity to monitor and store private communications.

Secondly, various states have tried to curtail citizens' access to foreign sites because they clash with their national laws, even while those sites are perfectly legal in their country of publication. In France, a group of anti-racism activists started a lawsuit against the US provider Yahoo! for auctioning Nazi memorabilia on its pages. Yahoo! was sued in France for what was perfectly legal within US law and for pages that they served from the US. Nevertheless, Yahoo! lost the case: judge Jean-Jacques Gomez, in an appeal ruling issued in November 2000, reaffirmed that Yahoo! had to prevent French web surfers from accessing those pages and basically ordered Yahoo! to start country-by-country filters. (13)

As the UK based organization Internet Freedom wrote about the case: "If courts deem material on Web sites hosted in other countries to be unacceptable to their citizens and block them from viewing it [..] they will have to take into account the mores and legislation of every country. Any number of filtering regimes will have to be initiated to enable them to comply with whatever restrictions and legislation they are faced with. This will make running what are already complex operations an almost impossible task. This case sets a precedent in that a court has decided to apply its national law to a Web site based in another country. The decision challenges the Net as a universal, borderless medium. It paves the way for a Net that will be regulated to the lowest common denominator in order for content providers to avoid the possibility of legal action. A global communications medium now faces the distinct possibility of decisions about what can be placed on it decided by the most reactionary of regimes. Center for Democracy and Technology analyst Ari Schwartz said: 'If (US Web sites) have to follow 200 country laws, then (they) would have to follow the one that allows the least (freedom of) speech. What if Saudi Arabia said it was concerned about people posting pictures of women with their heads uncovered?'" (14)

After this appeal ruling, Yahoo! wisened up and started procedures of its own in the US. In November 2001, a US District Court ruled that the French court order regarding Internet content is unenforceable in the US because it violates the First Amendment's guarantee of free speech. The court granted broad protection to US websites engaged in constitutionally protected activity, but stated that website operators may nevertheless for practical reasons decide to comply with conflicting foreign law requirements. It further stated that only treaties and other international legal mechanisms lay the ground for the resolution of conflicts between different legal regimes applicable to the Internet. (15)

But this is precisely what will start happening. The Cybercrime Convention that came into being in November 2001 – and which has been signed by, amongst others, the US, Canada, Japan and many European countries, "formalizes the notion of extra-territorial action by a party in one country objecting to content on a Web site based in another country. Article 23 of the convention creates supra-national reach for each signatory state. Even if a signatory state's legal system does not have the procedure to apply a request made by another signatory, under article 27 this is not seen as sufficient grounds to refuse that request. The consequence of this is that signatory states can be forced to act beyond their means and in contradiction to their own legal system." (16)

Meanwhile, in March 2001 a German court had already announced that it would *not* prosecute Yahoo! over a similar complaint filed against it in that country. However, that was

not because Germany respects the fact that it has no jurisdiction over foreign sites; the court merely reasoned that "while Germany has some of the strongest laws against hate literature in the world, the German court reportedly recognized Yahoo! as an Internet service provider and, as such, [it] ruled [that] the company should not be held liable for the content of its auction Web sites." (17)

This policy of the courts does not necessarily match that of the country or its federal states, and – as we just saw – the new Cybercrime Convention *does* allow for different local laws being applied to web pages. (18) And indeed, in March 2002, the German federal state of North Rhine-Westphalia decided that two right wing extremist sites hosted in the United States – www.stormfront.org and www.nazi-lauck-nsdapao.com – must be blocked, and ordered some 80 ISPs and universities to block access to those sites. Many computer literate people in Germany fear that this censorship will not stop there:

"Fighting right wing extremist ideologies reaches a broad consensus in Germany; however in this case it is used to gain acceptance for the establishment of a nationwide centralized filtering and blocking system," wrote a protesting committee. "Future plans contain blocking of content to protect minors, copyrights and consumer rights, including search engines that fail to accord with corresponding national guidelines and laws. Together with corporate partners, the North Rhine-Westphalia administration is developing a high capacity filtering system that is currently being tested at the University of Dortmund. The intention is to create a framework with centrally controlled blocking mechanisms that should be installed on gateway machines to the 'foreign Internet'." (19)

The main questions are, however, not dealt with by filtering. Why should people be prevented from seeing sites like this in the first place? Will racism stop simply because you cannot read hate sites? Is it better to block such sites than to argue their content?

Legal Sites and Economic Profit

While individual Internet users are starting to suffer from countries trying to impose their national laws upon one another, a new problem has arisen: upstream providers pulling the plug on ISPs because of legal but disputed material.

All ISPs have an upstream provider, who sells them bandwidth. Companies who provide collocation – either in the form of rented web space or in the form of web servers located there – have upstream providers, too. And upstream providers often have their own upstream providers. Currently, at the top of the chain there is only a handful of US backbone providers, plus one or two single players.

Flashback was both a magazine and a small provider in Sweden. The magazine was known for its free-speech stance. They started their provider services in 1996, just before the big Internet craze hit the country. Users got both free web space and a free e-mail address after subscribing to the magazine. Among the more than 50,000 sites hosted on Flashback, was one containing Nazi propaganda, carefully phrased so as to not violate Swedish law. That particular page was nevertheless reported to the prosecutor, who after investigation decided that they were indeed well within the boundaries of Swedish law. There simply was no case against Flashback, nor against that one user.

In the course of 2000, Björn Fries – an alderman of the Swedish city Karlskrona, and a prominent anti-Nazism fighter – started a campaign against Flashback because of this right-

wing user page. Flashback insisted on their free speech policy and refused to remove pages that had already been deemed legal. Fries then turned to Flashback's upstream provider, Air2Net, which in turn was a subsidiary of the US company MCI/Worldcom. Fries managed to rally other downstream providers of both Air2Net and MCI/Worldcom against those pages. Fearing a commercial setback, MCI/Worldcom decided that Flashback had either to pull those pages, or they would pull the plug on both Flashback *and* Air2Net, which of course vastly increased the pressure on Flashback. Flashback however kept its stance and was then disconnected: thousands of users suddenly lost their homepages and their e-mail accounts, simply because a US company didn't want to lose customers over a disputed but legal page. (20) Flashback tried several other upstream providers, but as it turned out, *all* of them were dependent upon MCI/Worldcom.

In a case like this, what does your constitutional right not to be censored entail? European national laws allow people their day in court: every citizen is given the opportunity to put his publication before a judge and let the court decide. But here, no court was invoked; actually, the prosecutor has stated that these pages were provocative but completely within legal limits. It was a US based multinational who decided what you can publish and what not.

Something similar happened in the Netherlands. Xtended Internet, a small Dutch provider, hosts a website which is under attack by Scientology. (21) At the end of 2001, Xtended Internet's upstream provider, Cignal, received a complaint. It was from Scientology, claiming copyright infringement on www.xenu.net's pages. Xtended Internet and the maintainer of www.xenu.net refuted the complaint, but despite that, Xtended Internet was notified that Cignal's own upstream provider, the US based company Priority Telecom, had booted Xtended Internet. Again, a whole provider went down over a page that appeared to be perfectly legal. (22)

As Paul Wouters of Xtended Internet put it: "We were disconnected even after proving that disconnecting or censoring our customer would violate Dutch case law. We voluntarily agreed to follow the DMCA, (23) so as to make it easier for Cignal to get out of this conflict, even though US law, and thus the DMCA, didn't apply to us. Yet, Cignal chose the easy way out. Obviously we were not worth the money that Scientology's lawyers could cost them. And maybe that is what frightens me most. Not that they don't care about freedom of speech issues, but that they have censored us solely based on commercial reasons. Censorship has become a profitable business and the freedoms that are granted to us by the Dutch constitution are revoked at the stroke of a pen by American corporate lawyers." (24)

Old Media Versus New Media

In Italy, a remarkable fight developed between "traditional" journalists and Internet journalism. Shortly after World War II, in 1948, Italy introduced a national law on the press. According to that law, all published periodicals have to give to the Tribunal (the local district court) the name of a "responsible director", who in turn has to be member of the National Order of Journalists. Registration costs about 200 dollars. Additionally, all periodicals are obliged to print the name and address of their editor and printer.

The National Order of Journalists – which poses quite a powerful body in Italy – was rather suspicious of the development of Internet journalism, and undertook a lobby for Internet publications to be brought under the scope of the existing law. The new law was

adopted in April 2001. The NJO lobby forced big portals (such as Kataweb-Repubblica, Rai.it, Supereva, etc.) to recognize the "journalist profession" and, subsequently, to remunerate hundreds of people who work like their colleagues, but have less job security. (25)

What started as an attempt to extend state subsidies to Internet media, basically brought those publications under the 1948 press law. And the new law itself is, as Interlex – an Italian web magazine about law, technology and information – put it, "confused and confusing […] the law is shameful, its rules absurd". A strict interpretation of the law defines "every Italian web site geared to transmit information towards the public" as an "editorial product" and subjects it to the regulations of the law. (26)

And more fundamentally, the law is impossible to live up to, due to technical flaws: the obligation to state the name and address of the printer, while there *are* no printers on the Net and people usually do not know on which server their pages are hosted, least of all the physical location of that server. Additionally, the law claims jurisdiction over Internet publications that are hosted on foreign servers.

While it seems unlikely that websites that are not producing regular news and information will be forced to register, it is highly possible that websites like Indymedia will, and will have to give the name of a "responsible director" and a "printer". Many people fear that this law will indeed be used to weed out publications that are outside the currently accepted framework.

Turkey is currently debating a similar law.

Spain is on the verge of approving one too, in May 2002. The bill for the "Law of Information Society Services and Electronic Commerce" (*Ley de Servicios de la Sociedad de la Informacion y de Comercio Electronico*, known by its Spanish acronym LSSI) plans to force websites to register with the Government and require web hosting companies to police content by reporting suspected illicit activity. (27) Apart from that, the upcoming law will allow a "competent administrative authority" in Government to shut down websites unilaterally; a power that now requires court approval. In Spain, only a judge can ban printed press editions from the news stands, but under the LSSI, an official could "provisionally" ban the edition of an on-line publication if it "outrages or *could* outrage" values protected by the law, while the paper version of the same publication still enjoys constitutional protection. (28)

If any such measures were to be imposed on other media, people would be outraged. With the Net, these kind of measures are often accepted without questioning. Civil liberties organizations fear that limiting Internet publication freedoms is only a first step towards curtailing other media; after all, once a measure is accepted in one area, it is difficult to stop it in another.

Freedom of the Internet, Our Concern

Seeing the amount of effort that Western countries are making to filter content on the Web, it is only a matter of time before other countries catch up. Meanwhile what we are seeing is more and more countries placing Internet publications and private communications under greater scrutiny and passing laws that restrict digital publications more than analogue ones – in part because they fear the anarchy that the Net once was and in part because it suddenly has become technologically feasible.

Networked computers allow for novel uses, unthinkable in the analogue world. They can be used to circumvent censorship and monitoring. But the Internet can also be used to scrutinize publications and communication to a degree that goes way beyond Orwell's wildest imagination.

Karin Spaink is a professional writer (homepage at http://www.spaink.net)
and works as an external expert for OSCE-FOM.
Christiane Hardy works as a Senior Advisor for the OSCE, for the
Freedom of the Media Office (http://www.osce.org/fom/)

Notes

1. "First, materials going into the home are more heavily censored than those going into the corporate world. [..] Information for the home is seen to be of a less critical nature so censorship of such information is regarded to have not as deleterious an effect. Second, materials for the young are more heavily censored than those for adults. This is an admittedly paternalistic principle of protecting the weaker members of society from the possible harm of the materials in question. [..] Third, materials for public consumption are more heavily censored than those for private consumption. This is a corollary of the second principle as it is assumed that the public includes those who are "weaker." [..] It should be noted that private consumption of censorship materials is still policed in that those found in private possession of censored materials can be convicted in court. Finally, materials deemed to have artistic and educational merit are less heavily censored." See Dr. Peng Hwa Ang and Ms. Berlinda Nadarajan, *Censorship and Internet: a Singapore Perspective.*
2. See *Defeating Singapore Internet Censorship - How to*, to be found at http://www.geocities.com/Pentagon/Barracks/8845/singapore_internet_censorship.html
3. See George d'Arnaud, *Internetbeperkingen in Dubai*, 10 November 1997, in the newsgroup xs4all.general, message-ID: <34698854.1990690@news.xs4all.nl>. The ensuing discussion proved that it was rather difficult – and takes quite some technical knowledge – to circumvent this national censorship rule.
4. Quoted from "New service to censor Internet", *The Gulf Today*, 25 January 1997.
5. Electronic Frontiers Australia Inc., Media Release of 7 September 2000: *Government Net Censorship Reports - Facts or Fallacies?,* http://www.efa.org.au/Publish/PR000907.html .
6. The full text of the CDA is at http://www.eff.org/Censorship/Internet_censorship_bills/ Amongst others, the CDA limited access to the King James Bible, Tarantino film scripts, lyrics by many pop groups, information about safe sex and breast cancer, and pictures of Michelangelo's David. The Supreme Court's ruling warned about the CDA's "obvious chilling effect on free speech [..] it unquestionably silences some speakers whose messages would be entitled to constitutional protection." The complete ruling can be found at http://www2.epic.org/cda/cda_decision.html .
7. *Radikal* was put on-line at http://www.xs4all.nl/~tank/radikal/ . The index page also contains a brief history of the German efforts to censor these pages. Unfortunately, many links to press releases and newspaper articles do no longer work.

8. For an overview of the debate regarding mandatory filtering systems, see the compilation provided by the Massachusetts Institute of Technology at http://www.mit.edu:8001/activities/safe/safe/labeling/summary.html and the news and resources provided by the Internet Free Expression Alliance (IFEA) at http://www.ifea.net
9. §§§See *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library*, 23 November 1998 http://www.techlawjournal.com/courts/loudon/81123op.htm . The COPA bill is currently being brought to the Supreme Court by the ACLU, on the grounds that it is against the US First Amendment. See http://www.aclu.org/court/beeson_01.html
10. The US Congress passed the *Children's Internet Protection Act* on 15 December 2000. The full text of the act is at http://www.ifea.net/cipa.html
11. Complaint filed in Philadelphia, 20 March 2001.
12. *European Parliament resolution on the existence of a global system for the interception of private and commercial communications (ECHELON interception system),* (2001/2098(INI)), released on 9 June 2001. Full text at http://www3.europarl.eu.int/omk/omnsapir.so/pv2?PRG=DOCPV&APP=PV2&LANGUE=EN&SDOCTA=21&TXTLST=1&POS=1&Type_Doc=RESOL&TPV=PROV&DATE=050901&PrgPrev=TYPEF@A5|PRG@QUERY|APP@PV2|FILE@BIBLIO01|NUMERO@264|YEAR@01|PLAGE@1&TYPEF=A5&NUMB=1&DATEF=010905 .
13. For a concise article about the case, see "Court to Yahoo: Use Nazi Filter", in *Wired*, 20 November 2000, http://www.wired.com/news/politics/0,1283,40285,00.html .
14. Dave Amis: "The Net now has a national court: this month it's French!", in *Internet Freedom*, 9 January 2001, http://www.netfreedom.org/news.asp?item=137 .
15. §§§A summary of the ruling is at http://www.ffhsj.com/bancmail/pdf/011120.pdf .
16. Dave Amis, op. Cit.
17. Jay Lyman, "German Court Rules Yahoo! Not Liable For Nazi Auctions", in *NewsFactor Network*, 28 March 2002, http://www.newsfactor.com/perl/story/8500.html .
18. §The Cybercrime Convention ("*Draft convention on cyber-crime and explanatory memorandum related thereto*") as accepted by the Council of Europe can be found at http://www.privacyinternational.org/issues/cybercrime/coe/cybercrime-final.html . Comments and criticisms are at http://www.privacyinternational.org/issues/cybercrime/ .
19. Joint press release from Chaos Computer Club and ODEM.org, to be found at http://www.politechbot.com/p-03318.html . For more information, see also http://www.odem.org/informationsfreiheit/en/ , http://www.netzzensur.de/index_en.html and Alexander J. Kleinjung, "Vom Daten-Highway auf die Straße", in the German edition of *CT*, 2002/9.
20. Flashback <http://www.flashback.se> is currently up again, but now only as a news agency. A list of news articles about the shutdown is available through Flashback's mirror at http://fb.provocation.net/www.flashback.se/ .
21. See http://www.xenu.net . While Scientology has repeatedly threatened Andreas Heldal-Lund, the owner of the website, they have at the same time abstained from any legal action against him. Instead, Scientology chooses to threaten providers hosting the site, and their upstream providers.
22. The history of Xtended Internet's contracts and correspondence with Cygnal is documented at http://www.xtdnet.nl/paul/PriorityTelecom-Xenu.html .

23. The DMCA is a US law to deal with digital copyright infringement. Scientology invoked this US law, even though Xtended Internet is Dutch and the maintainer of ww.xenu.net is Norwegian. Hence, the DMCA does not even apply in this case.
24. Paul Wouters, at http://www.xtdnet.nl/paul/PriorityTelecom-Xenu.html .
25. See the description by Snafu at http://amsterdam.nettime.org/Lists-Archives/nettime-l-0202/msg00109.html .
26. Manlio Cammarata, "Qui succede un 'quarantotto'", in *Interlex*, 4 April 2001, http://www.interlex.it/stampa/48.htm .
27. Julia Scheeres, "Fears of a Website Inquisition", in *Wired*, 29 May 2001, http://www.wired.com/news/business/0,1367,44110,00.html .
28. Steve Kettmann, "Spanish Web Law Sparks Debate", in *Wired*, 1 May 2002, http://www.wired.com/news/print/0,1294,52201,00.html .