CHAPTER 10

Web of People

The Web is more a social creation than a technical one. I designed it for a social effect—to help people work together—and not as a technical toy. The ultimate goal of the Web is to support and improve our weblike existence in the world. We clump into families, associations, and companies. We develop trust across the miles and distrust around the corner. What we believe, endorse, agree with, and depend on is representable and, increasingly, represented on the Web. We all have to ensure that the society we build with the Web is of the sort we intend.

When technology evolves quickly, society can find itself left behind, trying to catch up on ethical, legal, and social implications. This has certainly been the case for the World Wide Web.

Laws constrain how individuals interact, in the hope of allowing society to function. Protocols define how computers interact. These two tools are different. If we use them correctly, lawyers do not tell computer programmers how to program, and programmers

do not tell legislators how to write laws. That is on an easy day. On a difficult day, technology and policy become connected. The Web Consortium tries to define protocols in ways that do not constrain the norms or laws that govern the interaction of people. We define mechanism, not policy. That said, it is essential that policy and technology be designed with a good understanding of the implications of each other. As I noted in closing the first International World Wide Web Conference at CERN in May 1994, technologists cannot simply leave the social and ethical questions to other people, because the technology directly affects these matters.

Since the Web is a work in progress, the consortium seeks to have a dialogue with policy makers and users about what sort of social interactions the Web should enable. Our goal is to assure that the Web accommodates the maximum diversity of public policy choices. In areas like freedom of expression, privacy, child protection, intellectual property, and others, governments do have a role. The kinds of tools we make available can help assure that those laws are effective, while also ensuring that individuals retain basic control over their online experience.

Through 1996, most of what happened to the Web was driven by pure excitement. But by 1998, the Web began to be seen as a battleground for big business and big government interests. Religious and parental groups began to call for the blocking of offensive material on the Web, while civil rights groups began to object strongly to these objections. For this reason, among others, many people in business, government, and society at large would like to "control" the Web in some way.

Unfortunately, these power plays are almost all we hear about in the media: the Justice Department's antitrust case against Microsoft, the merger mania and soaring stock prices of Internet companies, and the so-called battle of the portals—the attempts by mammoth Web sites such as Yahoo!, service providers like America Online, and content companies like Disney to provide the widest window to the Web's content.

While these maneuvers certainly affect the business of the Web, in the larger picture they are the background, not the theme. Some companies will rise, some will fall, and new ones might spring from the shadows and surprise them all. Company fortunes and organizational triumphs do not matter to our future as Web users nearly as much as fundamental sociotechnical issues that could make or break the Web. These have to do with information quality, bias, endorsement, privacy, and trust—fundamental values in society, much misunderstood on the Web, and alas highly susceptible to exploitation by those who can find a way.

Bias on the Web can be insidious and far-reaching. It can break the independence that exists among our suppliers of hardware, software, opinion, and information, corrupting our society. We might be able to hold bias in check if we all could judge the content of Web sites by some objective definitions. But the process of asserting quality is subjective, and is a fundamental right upon which many more things hang. It is asserted using systems of endorsement, such as the PICS protocol the consortium developed to show that government censorship was not necessary. The large number of filtering software tools now available show that government censorship is not even as effective: A nation's laws can restrict content only in that country; filters can block content no matter where it comes from on the Web. Most important, filters block content for users who object to it without removing the material from the Web. It remains available to those who want to see it.

I would like to see similar endorsement techniques used to express other subjective notions such as academic quality.

The essence of working together in a weblike way is that we function in groups—groups of two, twenty, and twenty million. We have to learn how to do this on the Web. Key to any group's existence is the integrity of the group itself, which entails privacy and confidentiality. Privacy involves the ability of each person to dictate what can and cannot be done with their own personal

information. There is no excuse for privacy policies not to be consensual, because the writing, checking, and acceptance of such policies can all be done automatically.

Agreements on privacy are part of the greatest prerequisite for a weblike society: trust. We need to be able to trust the membership of groups, the parties engaging in e-commerce, the establishment of who owns what information, and much more. Nowhere is the difference between the old tree-oriented model of computing and the web model more apparent—and nowhere is society so completely tied to technology—as the online structure that decides who and what we trust. The criteria a person uses to assign trust can range from some belief held by their mother to a statement made by one company about another. Freedom to choose one's own trust criteria is as important a right as any.

A key technology for implementing trust is *public key cryptography* (PKC), a scheme for encoding information so no one else can read it unless he or she has the key to decode it. How we can use it directly affects what we can do socially. With this tool, we can have completely confidential conversations at a distance—vouch for the authenticity of messages, check their integrity, and hold their authors accountable. However, it is not available, largely for political reasons explained in the next chapter.

For all its decentralized growth, the Web currently has one centralized Achilles' heel by which it can all be brought down or controlled. When the URI such as http://www.lcs.mit.edu/foo is used to find a web page, the client checks the prefix, and when, as often, it is "http" it then knows that the www.lcs.mit.edu part is the "domain name" of a Web server. The domain name system runs on a hierarchical set of computers, which may be consulted to find out the actual Internet address (one of those numbers like 18.23.189.58) to which packets may be sent. At the top of the hierarchy are five computers that store the master list—and an

operator error on one of them did once black out the system, causing huge disruption. That technical weakness is itself less of a concern than the social centralization that parallels it.

Both the domain names and the Internet addresses are given out in a delegated way. To set up the name www.lcs.mit.edu, one registers it with the Lab for Computer Science, which is owner of the lcs.mit.org domain. LCS got its domain name in turn from MIT, which is the registered owner of mit.edu. MIT got its domain from the owner of edu. Control over the "top-level" domains such as .com and .edu indirectly gives control over all domain names, and so is something of great power. Who should exercise that power?

During the entire growth of the Internet, the root of an Internet address was administered by a body known as the Internet Assigned Numbers Authority. IANA was set up, was run by, and basically *was* the late Jon Postel, an Internet pioneer and guru at the University of Southern California. Jon managed IANA as a public trust, a neutral party. Much of the growth of the Web and Internet depended on his integrity as the ultimate trusted authority who saw to it that the delegation of domain names was fair, impartial, and as unfettered as possible. Because of the sort of person Jon was, it worked. The Web and Internet as a whole owe a lot to Jon, who died in October 1998 at age fifty-five.

Potential problems of unfair control over domain names loomed larger when the U.S. government decided in late 1998 that IANA should be privatized. The potential problem was exacerbated by URI prospectors. The registration of domain names had always been done on a first-come, first-served basis. Increasingly, everyone realized that short, memorable URIs were valuable commodities; the scramble for recognizable domain names, like *candy.com* and *gamble.net*, reached fever pitch. Speculators began to register any name they could think of that might someday be worth more than the one-hundred-dollar registration fee. Domain names like *soap.com* and *sex.com* were snapped up, in

hopes of later holding out for a lucrative offer. Select names have since changed hands for large sums of money.

One problem is that the better domain names will wind up with the people or companies that have the most money, crippling fairness and threatening universality. Furthermore, the ability to charge for a domain name, which is a scarce, irreplaceable resource, has been given to a subcontractor, Network Solutions, which not surprisingly made profits but does not have the reputation for accountability, or meeting its obligations. It is essential that domain names be primarily owned by the people as a whole, and that they be governed in a fair and reasonable way by the people, for the people. It is important that we not be blind to the need for governance where centralization does exist, just because the general rule on the Internet is that decentralization makes central government unnecessary.

Technically, much of the conflict is due to the mismatch between the domain name structure and the rules of the social mechanism for dealing with ownership of names: the trademark law. Trademark law assigns corporate names and trademarks within the scope of the physical location of businesses and the markets in which they sell. The trademark-law criterion of separation in location and market does not work for domain names, because the Internet crosses all geographic bounds and has no concept of market area, let alone one that matches the existing conventions in trademark law. There can be a Joe & Sons hardware company in Bangor, Maine, and a Joe & Sons fish restaurant in San Francisco. But there can only be one joeandsons.com.

Whatever solution is found must bridge the gap between law and technology, and the chasm is fairly wide. Suppose a commercial entity is limited to just one domain name. Although under those circumstances it might be hard to manage the persistence of domain names when companies changed hands, companies also might be prevented from snapping up names with every English word related to their area of business. There are some

devices in the existing domain name system that can ease the problem. For example, if a widget company in Boston can't get the name *widget.com* because it's already taken, it could try the geographically based name *widget.boston.ma.us*.

A neutral, not-for-profit organization to govern the domain-naming process is currently being put together by the community at large. The original U.S.-centric nature of the domain name service has worried some non-Americans, so any new body will clearly have to be demonstrably international.

There has been a working proposal to create new *top-level domains*—the *.com* or *.org* or *.net* suffixes on domain names. This would add top-level domains for distinct trades, such as *.plastics*. In this way, *jones.plastics* and *jones.electrical* could be separate entities, easing the crush a little. However, the effect would be a repeat many times over of the ridiculous gold rush that occurred for *.com* names, making it necessary for holders of real trademarks to protect themselves from confusion by registering not just in three domains (*.com*, *.org*, and *.net*) but in many more. Unless it was accompanied by a legal system for justifying the ownership of a name on some real grounds, such a scheme would hurt everyone—except those standing on the sidelines ready to make a fast buck by grabbing names they never intend to use.

This is a relatively isolated problem with the Web, and one the W3C has stayed almost completely clear of to date. It does serve as a good illustration of the way a single centralized point of dependence put a wrench in the gears of an otherwise smoothly running decentralized system. It also shows how a technical decision to make a single point of reliance can be exploited politically for power and commercially for profit, breaking the technology's independence from these things, and weakening the Web as a universal space.

Even without a designed-in central point, the Web can be less neutral, and more controlled, than it may seem. The Web's infrastructure can be thought of as composed of four horizontal layers;

from bottom to top, they are the transmission medium, the computer hardware, the software, and the content. The transmission medium connects the hardware on a person's desk, software runs Web access and Web sites, while the Web itself is only the information content that exists thanks to the other three layers. The independence of these layers is important. From the software engineering point of view, this is the basic principle of modularity. From the point of view of economics, it is the separation of horizontal competitive markets from anticompetitive vertical integration. From the information point of view, think of editorial independence, the neutrality of the medium.

The Microsoft antitrust case was big news in 1999, much of it an argument about the independence in the software layer of an operating system and a browser. In the same year, scarcely a month went by without the announcement of a proposed merger or acquisition between large companies. Two types of deals were taking place, the first between companies that carry data over phone and cable TV lines, the second between content providers. Each of these deals was happening within one of the Web's layers.

I am more concerned about companies trying to take a vertical slice through the layers than creating a monopoly in any one layer. A monopoly is more straightforward; people can see it and feel it, and consumers and regulators can "just say no." But vertical integration—for example, between the medium and content—affects the quality of information, and can be more insidious.

Keeping the medium and the content separate is a good rule in most media. When I turn on the television, I don't expect it to deliberately jump to a particular channel, or to give a better picture when I choose a channel that has the "right" commercials. I expect my television to be an impartial box. I also expect the same neutrality of software. I want a Web browser that will show me any site, not one that keeps trying to get me to go back to its host site. When I ask a search engine to find the information it can on a topic, I don't expect it to return just the sites of compa-

nies that happen to advertise with or make payments to the search engine company. If a search engine is not giving me completely neutral results, then I should be told about it with some notice or icon. This is what magazines do when they run an "article" that has been paid for by an advertiser; it is labeled "advertorial," or "special advertising section," or some such thing. When companies in one layer expand or merge so they can cross layers, the potential for undermining the quality of information in these ways increases greatly.

The trouble begins when a program that an individual depends on for his use of the Web, such as an operating system or browser, displays an array of icons that will automatically connect him to preferred search engines, Web sites, online programs, or ISPs. Such arrangements become more troubling if a user gets a single browser/operating system that is written as one integrated software program, and cannot remove such links or negotiate independent arrangements with other providers of similar services that will work with the browser/operating system.

Even the hardware companies are getting into the act. In 1998, Compaq introduced a keyboard with four special keys: hitting the Search key automatically takes the user to the AltaVista search engine. Suddenly, where a person searches the Web depends on where he bought his computer. A user does not know where he stands when he hits a "Search the Web" or "Best of the Web" button on a browser or a keyboard. These buttons or keys take the user into a controlled view of the world. Typically they can be set by the user to point to any search engine—but few users change the default.

More insidiously still, it could also be possible for my ISP to give me better connectivity to sites that have paid for it, and I would have no way of knowing this: I might think that some stores just seemed to have slow servers. It would be great to see some self-regulation or even government regulation in these areas.

The Web's universality leads to a thriving richness and diversity. If a company claims to give access to the world of information, then presents a filtered view, the Web loses its credibility. That is why hardware, software, and transmission companies must remain unbiased toward content. I would like to keep the conduit separate from the content. I would like there always to be a choice of the unbiased way, combined carefully with the freedom to make commercial partnerships. And when other people are making a choice for me, I would like this to be made absolutely clear to me.

Some might argue that bias between the layers is just the free market in action. But if I bought a radio and found that it accessed only certain stations and not others, I'd be upset. I suppose I could have a half dozen radios, one for each set of stations. It makes no more sense to have a half dozen computers or different operating systems or browsers for Web access. This is not just impractical; it fragments the Web, making it cease to be universal. I should be able to buy whichever computer, software, and transmission service I want and still have access to the entire content of the Web.

The portals represent the self-reinforcing growth of monopolies, especially those that integrate vertically. In its greater context, the battle of the portals is a battle for brand names on the Web. It is difficult for someone to judge the quality of information, or Web software and services, without extended experience and comparison. As a result, software or transmission companies with existing reputations can capitalize by using their names to attract people to their information services. The extreme would be a company that offered transmission, hardware, software, and information, and then tried to brand itself as more or less equivalent to the Web. It would also be a repeat of the dial-up service world of AOL and CompuServe that existed before the Web, on a larger scale. So far, the urge to achieve dominance has driven the quality on the Web upward, but any one company's attainment of it would destroy the Web as we know it.

Happily, the Web is so huge that there's no way any one company can dominate it. All the human effort people and organizations have put in all over the world to create Web sites and home pages is astoundingly large, and most of the effort has to do with what's in the Web, not the software used to browse it. The Web's content, and thus value, will continue despite any one company's actions.

But consider what could happen in a year or two when search engines get smarter. I click the Search button on my keyboard, or tell a search engine, "I want to buy a pair of shoes." It supposedly heads out onto the Web to find shoe stores, but in fact brings me only to those shoe stores that have deals with that search engine or hardware company. The same with booksellers. Insurers. News. And so on. My choice of stores and services has thus been limited by the company that sells the computer or runs the search service. It's like having a car with a Go Shopping for Shoes button on the dashboard; when pushed, it will drive only to the shoe store that has a deal with the carmaker. This doesn't help me get the best pair of shoes for the lowest price, it doesn't help the free market, and it doesn't help democracy.

While there are commercial incentives for vertically integrating the layers into one business, legal liability can complicate the picture. In 1998 a Bavarian court convicted Felix Somm, a former head of the German division of CompuServe, of complicity in knowingly spreading pornography via the Internet. The two-year suspended sentence marked the first time in Germany that an online company manager had been held responsible for providing access to content deemed illegal. The material was obtained from computers in other countries, but through CompuServe's gateway to the Internet. When the boundary between the medium and the content is blurred, every ISP or telecommunications company is in danger of being liable for content.

Somm said he had even notified German authorities about the illegal material and aided them in their investigation. CompuServe also provided its subscribers with software they could use to block access to offensive material. Somm may have a chance for acquittal under a new German multimedia law that was passed after he was charged. It says that Internet service providers can be held responsible for illegal material on their servers only if they are aware of it, it is technically feasible to stop it, and they do not take reasonable measures to block access to it—which is what Somm and CompuServe said they did. Somm's defense attorneys argued that no one can be aware of everything on the Internet, and that blocking access to any one bit of it is an exercise in futility.

Since the Web is universal and unbounded, there's all sorts of junk on it. As parents, we have a duty to protect our young children from seeing material that could harm them psychologically. Filtering software can screen information under control of the reader, to spare the reader the grief of having to read what he or she deems junk. People use filters on e-mail to automatically categorize incoming information. An individual clearly has the personal right to filter anything that comes at him, just as he would do with regular mail: Some he opens, some he tosses into the garbage. Without this right, each day would be chaos. In the future, good browsers will be able to help the user avoid links to Web sites that have attributes he has indicated he doesn't want to have to confront, whether it's the presence of a four-letter word or the fact that the site shows ads.

But when someone imposes involuntary filters on someone else, that is censorship. If a library is supposed to provide a computer that gives citizens access to the Internet, but it prevents access to certain types of material such as pornography, then the library is deciding for the citizenry what they should be able to read. Here the library is installing itself as a central authority that knows better than the reader.

In 1998 patrons of the Loudon County, Virginia, public library filed suit seeking to remove a filter program installed on Internet computers at six county library branches. They claimed that, while the filter blocked them from accessing pornographic sites, it also blocked them from sites with information on sex education, breast cancer, and gay and lesbian rights. The principle here is more interesting than the bickering over details: The suit charged that the library's policy was an unconstitutional form of government censorship.

Just how thorny these qualitative decisions can be was illustrated by a 1998 case described in the *New York Times:* "The American Family Association, a conservative Christian group, has been a vocal supporter of filtering products. So it was with some surprise that officials at the group recently discovered that their own Web pages were being grouped with white-supremacist and other 'intolerant' sites blocked by a popular filter called Cyber Patrol. Researchers at Cyber Patrol decided the site met the filter's definition of intolerance, which includes discrimination based on sexual orientation." It seems researchers had found statements on the group's page that spoke out against homosexuality. Cyber Patrol bans up to twelve categories of material it considers inappropriate for the typical twelve-year-old, from gambling to cult sites.

The subjective nature of these decisions is why we set up the PICS system to allow anyone to customize their own objectives without imposing them on others. The key to PICS, and to any attempt to filter, is to give the reader control, and to make different filters available from different groups. With PICS, parents aren't limited to a given label provider, or even a given system of ratings. They have a range of commercially available surveillance programs to choose from—a choice of whom we trust.

The larger point to remember is that laws must be written in relation to actions, not technology. The existing laws that address illegal aspects of information are sufficient. Activities such as

fraud and child pornography are illegal offline and online. I don't like the idea of someone else controlling the kinds of information I can access. I do believe, however, that a parent has to protect his or her child on the Internet, just as they would guard where their child goes physically. But the decision as to what information adults can access needs to be up to them.

This principle was at the center of First Amendment disputes about the constitutionality of Internet censorship laws. When the first effort to censor the Internet was challenged in court, members of the consortium felt it was important that the courts understand how filters could act as an effective alternative to censorship. We provided background information during the deliberations. In 1996 the United States Supreme Court overturned the censorship law, in part because filters enable parents to protect their kids without requiring the government to step in and play nanny. But in 1998 Congress passed another censorship law. It's been challenged again, so that issue is far from settled.

The debate has become more complex, too. Some civil libertarian groups claim that repressive governments could use programs like PICS to squelch political or social communications on the Web that the government doesn't want read. One group, the Global Internet Liberty Campaign (GILC), wrote an open letter to the Web Consortium saying that, to avoid this danger, W3C should not release PICS Rules. PICS Rules is the part of the PICS technology that allows a person or group to store their preferences on a floppy disk, and give them to someone else to use. GILC was worried that the software for doing this could be misused by repressive governments against their own people. GILC also worried, according to Amy Harman of the *New York Times*, that if PICS technology was widely promulgated, Congress could pass a law requiring parents to adopt a particular set of PICS Rules. Since this would constitute government control, GILC said the consortium should not make PICS Rules a standard. We should just bury it.

Here the liberals seem to be wanting to leverage technology in order to constrain government. I find it troubling when Americans of any party don't trust their political system and try to go around it rather than get it right. The consortium is not going to prevent bad laws by selectively controlling what technology it develops and when to release it. Technologists have to act as responsible members of society, but they also have to cut themselves out of the loop of ruling the world. The consortium deliberately does this. It tries to avoid acting as a central registry, a central profit taker, or a central values setter. It provides technical mechanisms, not social policies. And that's the way it will stay.

The openness of the Web also means there must be a strong concern about business standards. Companies involved in electronic commerce are well aware of this, and some are making attempts to avoid possible governmental imposition of ethical standards by trying to regulate themselves, primarily with endorsements.

The Netcheck Commerce Bureau, for example, is a site where companies can register their commitment to certain standards, and receive a corresponding endorsement. Customers can lodge complaints against such companies with Netcheck. The long-established U.S. Better Business Bureau has a Web site that provides similar tools. Ideally, complaints to these sites will be monitored so that if a company doesn't do right by its customers, it will lose the seal of approval.

Some large companies are taking it upon themselves to establish what is in essence a branding of quality. Since the fundamental issue is determining which site to trust, if someone trusts a large company such as IBM, and IBM brands other companies as ethical, then the person will trust those companies, too. Indeed, IBM has developed what it calls an *e-business mark*, which it bestows on companies it does business with that have shown a commitment to delivering a secure and reliable environment for

e-commerce. It's like the Underwriters Laboratory symbol or the Good Housekeeping Seal of Approval.

Unlike regulation, endorsement can be done by anyone, of anything, according to any criteria. This three-way independence makes systems of endorsement very open. An individual can trust a product, or an endorser, or a particular endorsement criterion.

Self-regulation works when there is freedom to set different standards and freedom of consumer choice. However, if "self-regulation" simply becomes an industry version of government, managed by big business rather than by the electorate, we lose diversity and get a less democratic system.

The e-business mark may be a harbinger of the way many endorsements will go. People in general will not be able to figure out whether they trust a specific online store. So they'll resort to "trusted" brand names—or endorsements from them.

PICS was the consortium's mechanism to allow endorsements to be coded and checked automatically. It was aimed initially at showing that a Web site meets certain criteria for lack of nudity, violence, and such. It hasn't been implemented widely because there is no tremendous economic incentive for people to rate sites. But there may be a huge incentive when it comes to protecting the privacy of personal data someone gives to an online clothing store. The question is whose ratings, or settings, to trust.

As a consumer, I'd like to be made aware of the endorsements that have been given to a site—but without being distracted from the content. Perhaps icons could appear in a window I leave open while I access a site, or in the border around the page I'm viewing. Endorsements could be made in all fields, not just business. There could be academic endorsements: When I'm browsing through research papers on heart disease, an endorsement could appear that says a given paper has been published in a reputable journal. Each reader picks the journals he trusts. An individual would do the same with endorsements from associations in his profession. And if his medical association, say, happened to ignore

a particular branch of alternative medicine that he believes in, then he could use an endorsement that is based on a given journal of alternative medicine. That's the beauty of the Web; it's a web, not a hierarchy.

Endorsements, as a way of transmitting judgments of quality, work easily on the Web, because they can be made with hypertext links. However, important though this facility is, it is even more important to understand that a link does not have to imply any endorsement. Free speech in hypertext implies the "right to link," which is the very basic building unit for the whole Web.

In hypertext, *normal* links are between a hypertext document and another external document. *Embedded* links are those that cause something to appear with a document; a picture appears in a Web page because of an embedded link between the page and the picture. Normal hypertext links do not imply that the linked document is part of, endorsed by, or related in ownership to the first document. This holds unless the language used in identifying the contents of the linked document carries some such meaning. If the creator of the first document writes, "See *Fred's web page* [link], which is way cool," that is clearly some kind of endorsement. If he writes, "We go into this in more detail on our *sales brochure* [link]," there is an implication of common authorship. If he writes "Fred's *message* [link] was written out of malice and is a downright lie," he is denigrating (possibly libelously) the linked document. Clarifying the relative status of a linked document is often helpful to readers, but the person has to be responsible about what he says, just as he would in any medium.

For embedded links, however, the author of the document has responsibility, even if the contents have been imported from another Web site, and even if the document gives the URI for the embedded text or image so a browser can check the original source. If I write about the growth of the Web and show a graph, the graph is part of my document. It is reasonable to expect me

to take responsibility for the image just as for the text. They are logically part of the same document. Advertising embedded in a site is the exception. It would be great if the HTML distinguished links to "foreign" documents from links to documents with common authorship, and if browsers passed this information on to users in some way.

But beyond this distinction between normal and embedded links, certain misunderstandings still persist. Here are three myths that have crept into the "common wisdom" about the Web, and my opinion as to the way hypertext protocols should be interpreted.

MYTH ONE: "A normal link is an incitement to copy the linked document in a way that infringes copyright." The ability to refer to a document (or a person or anything else) is a fundamental right of free speech. Making the reference with a hypertext link is efficient, but changes nothing else.

Nonetheless, in September 1998, ABC News told the story of a photographer who tried to sue the department store JC Penny, which had a link from its site to the Movie Database Ltd. site, which in turn had a link to a Web site run by the Swedish University Network, which was said to have an illegally copied image of the photographer's. Fortunately, the suit was thrown out. A good default rule is that legality online is the same as it is offline. Users, information providers, and lawyers need to reach consensus on this. Otherwise, people will be afraid to make links for fear of legal implications. It would soon become impossible to even discuss things.

MYTH TWO: "Making a link to an external document makes the first document more valuable, and therefore is something that should be paid for." It is true that a document is made more valuable by links to other relevant, high-quality documents, but this doesn't mean anything is owed to the people who created those

documents. If anything, they should be glad that more people are being referred to them. If someone at a meeting recommends me as a good contact, does that person expect me to pay him for making reference to me? Hardly.

MYTH THREE: "Making a link to someone's publicly readable document is an infringement of privacy." The Web servers can provide ways to give Web site access only to authenticated people. This technology should be used, and Web site hosting services should give publishers control over access. "Security by obscurity"—choosing a weird URI and not telling people about it—is not conventional, and so a very explicit agreement must be made with anyone who is given the URI. Once something is made public, one cannot complain about its address being passed around.

I do feel it is right to have protection for confidential information that has become public by accident, illegal act, or force of law such as a subpoena. The current assumption that once information has "accidentally" escaped it is free to be used is unfortunate.

These are my personal feelings about how hypertext should be interpreted, and my intent. I am not an expert on the legalities in each country. However, if the general right to link is not upheld for any reason, then fundamental principles of free speech are at stake, and something had better be changed.