March, 1996

Mapping the Information Superhighway

Henry H Perritt, *Chicago-Kent College of Law*

Mapping the Information Superhighway

HENRY H. PERRITT, JR.[1]

1 Introduction

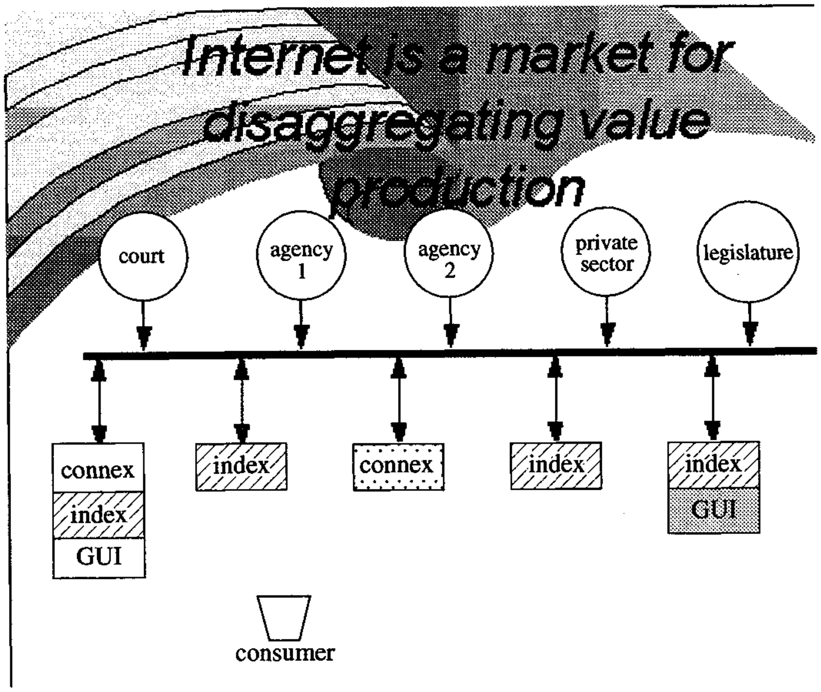
This paper[2] begins with an explanation of how new digital network technologies, sometimes referred to as the 'information superhighway', or the 'global information infrastructure', are best understood as a kind of market in which information products can be assembled from pieces supplied by many independent suppliers. Then it considers a number of issues that must be resolved to realize the potential of the information superhighway: can on open, distributed architecture like the Internet provide incentives for producing information value? Can open network architectures adequately protect security? Can technology enhance the signal to noise ratio? Can the legal profession ensure that public information remains publicly available?

2 The Importance of the Internet

Why is the Internet important? The Internet is important as a model for the Global Information Infrastructure(GII). The point is not that the present-day Internet represents the ultimate GII; the point is that today's Internet represents the kind of open, distributed network architecture that should represent the GII of the future. Because of its characteristics, the Internet is a market for disaggregating value production, and that characteristic has profound implications for the way commerce and democracy can operate and the way that legal institutions will function.

[1] Professor of Law, Villanova University School of Law, Villanova, PA 19085 Email perritt@law.vill.edu see also http://www.law.vill.edu

[2] This paper is adapted from a presentation given at the annual BILETA conference at the University of Strathclyde in Glasgow Scotland, April 1995.

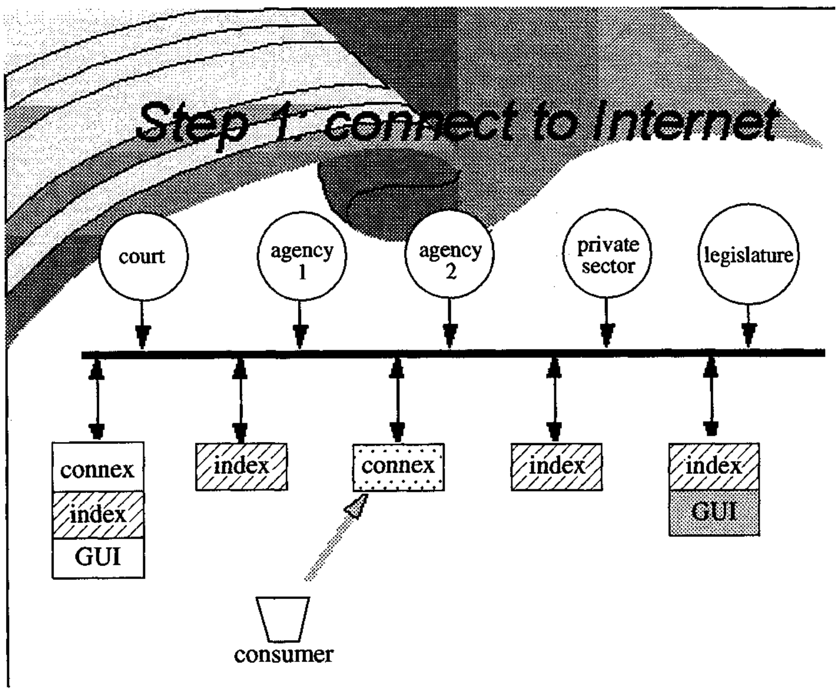


The chart represents the Internet by the dark line through the middle. Above the line, the circles represent sources of information content – just content; no added value features. Because of the Internet's open and distributed character, content originators can make their content available to other suppliers of information value and to ultimate consumers simply by placing their content in relatively raw form on computers called 'servers', and connecting those servers to the Internet.

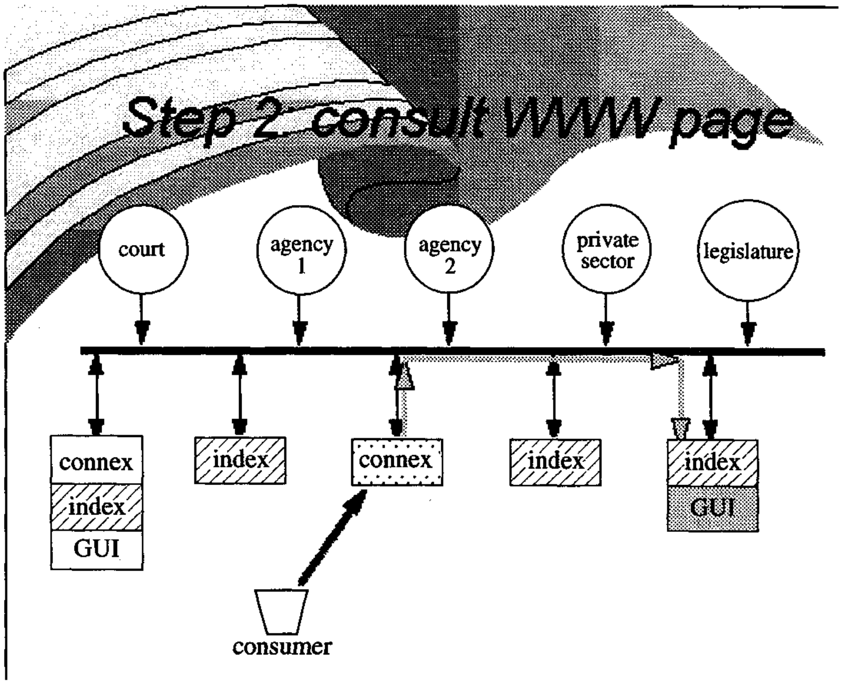
Then, other enterprises, public or private, represented in the figure by the rectangles below the solid line, can add value to the content supplied by the completely independent content originators. Moreover, suppliers of added value can specialize in only one or a few types of value. For example, in the figure, some producers, such as the one in the middle, supply only connection services. Others, like the second and fourth from the left, supply only indexing or pointers value. Other suppliers chose to bundle multiple types of value. The enterprise at the left supplies the combination of connection services, indexes and pointers, and graphical user interface software. The one at the bottom right supplies a combination of indexing and graphical user interface software value.

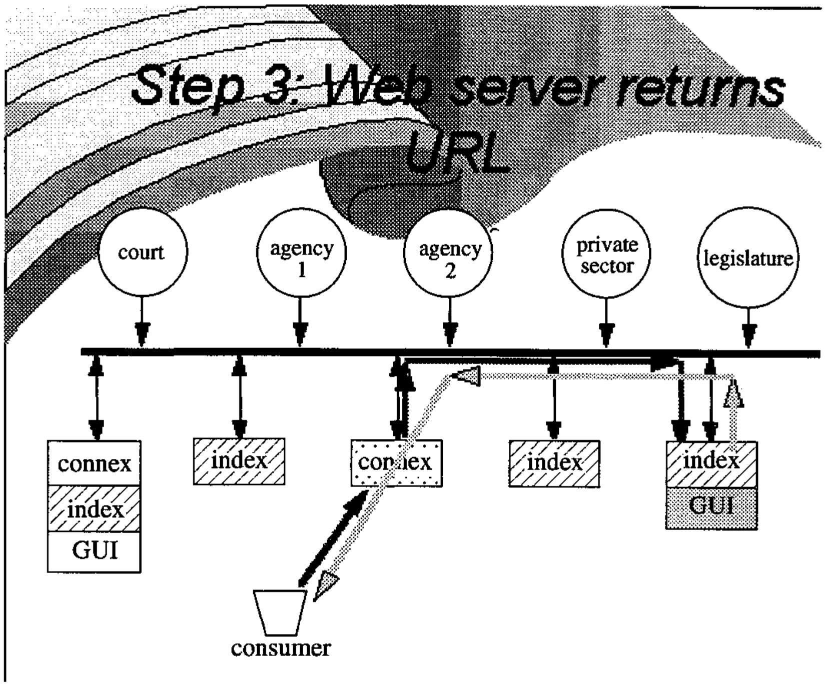
Internet applications such as the World Wide Web permit these independently supplied types of value to be combined through the Internet technical arrangements operating as a kind of market.

Figure 2 shows the first step in the assembly of the separate value added elements. A consumer wishing to obtain particular information content takes the first step by establishing a connection to the Internet through a provider of connection services.



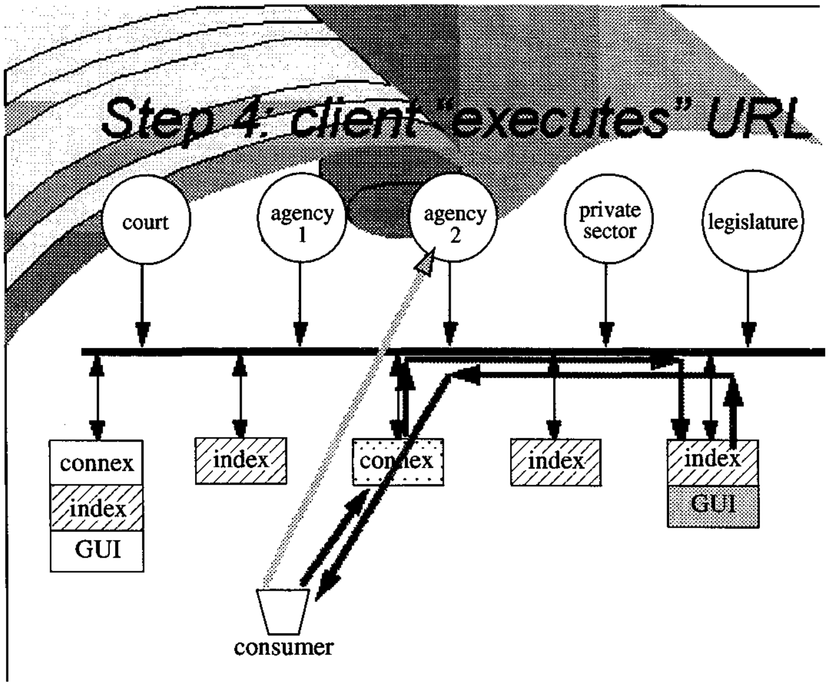
In step two (figure 3), the consumer establishes a further connection by specifying an Internet address or universal resource locator ('URL') or simply by selecting a bookmark on his World Wide Web browser. Regardless of the means of specifying the address, the consumer goes to a supplier of indexing value that the consumer knows points to the information that



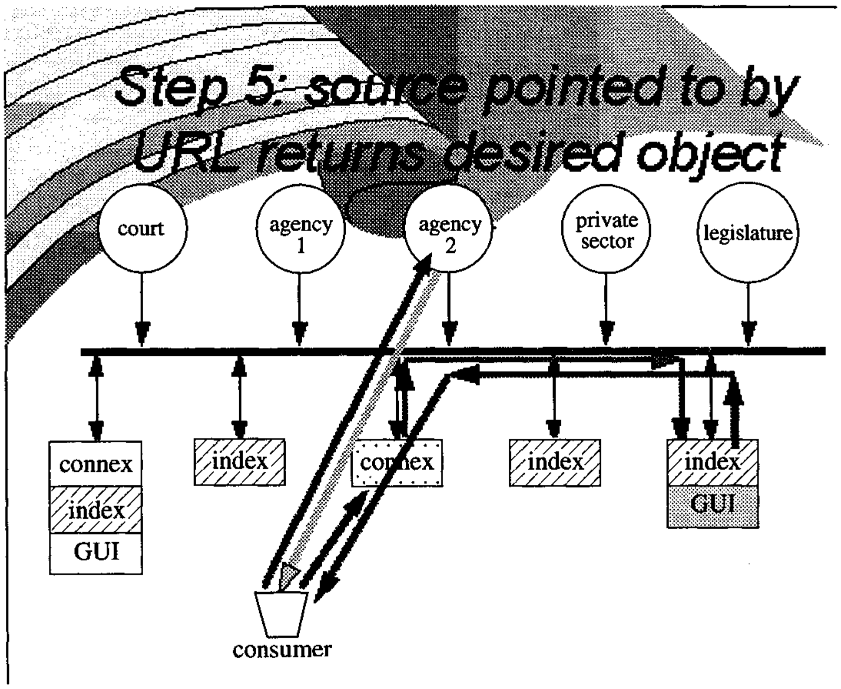


Step 3: Web server returns URL

interests him. For example, the consumer in the chart may have gone to the Villanova Center for Information Law and Policy which the consumer



Step 4: client "executes" URL



Step 5: source pointed to by URL returns desired object

knows has pointers to some 650 U.S. government sources, organized in its 'federal web locator'.[3]

In step three (figure 4), the user clicks on a particular pointer, say the one labelled 'the White House', and the World Wide Web server – the Villanova Center in the example – returns, not the content because it does not have the content, but instead returns a pointer to the desired information to the consumer's computer.

The consumer's computer, running 'Client' software in the form of a web browser like Netscape, executes the pointer, which causes a connection to be established with the content originator's computer, which actually contains the desired content.

The content server then returns the desired content, which may be a full text document, one or several images, or an audio or video file.

The aggregate of these distinct transactions is a value added information product assembled just in time to the specifications of a particular con sumer. This electronic assembly line is very different from the one associated with traditional print publishing which assembles bundles of information value in advance, for storage in a warehouse, just in case a consumer might want that particular bundle.

This is a powerful new possibility for information services. The unbundling greatly reduces barriers to entry for suppliers of all kinds, suppliers of content as well as suppliers of added value. Neither type of supplier

[3] http://www.law.vill.edu

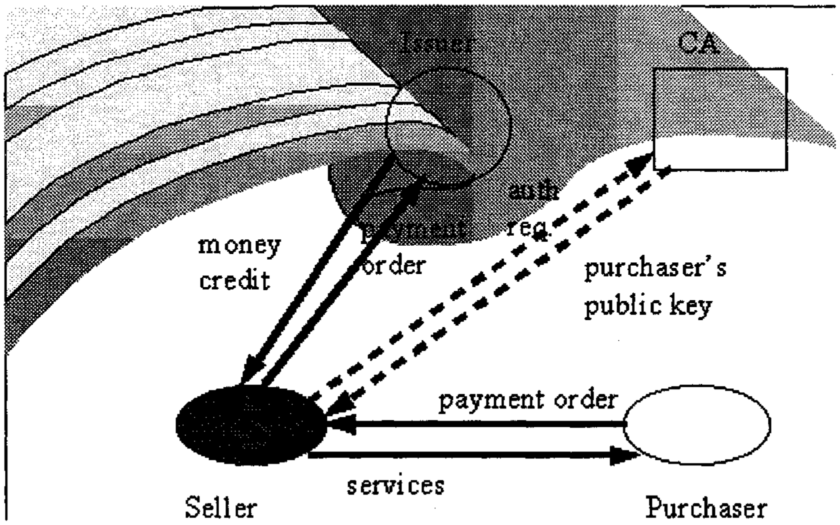
must raise the capital or have the wherewithal to supply complete bundles of information value. Because they can specialize, suppliers need less capital and confront lower operating costs. Reduced barriers to entry mean more competition and in the end more choice and lower prices for consumers and citizens.

But there are a number of issues that must be resolved before this vision becomes a reality for much of the world. First, can an open, distributed architecture like the Internet provide economic incentives for procedures of content and added value? Second, can open network architectures adequately protect security? Third, can technology enhance the signal to noise ratio? Fourth, can the legal profession ensure that public information remains publicly available?

3 Incentives for Producing Information Value

Despite the assertion that the Internet is a market for disaggregating value production, today's Internet is incomplete because it lacks payment mechanisms. While it is possible to make off-line payment arrangements, to deny consumers access to particular information objects or services unless they have made prior arrangements in writing or by telephone to establish accounts, requiring off line payment arrangements is cumbersome and slow. It defeats much of the potential of a real-time network for facilitating commercial transactions. Requiring advance payment arrangements for Internet transactions is as though one could order merchandise by telephone through a catalogue only if one wrote a letter first to establish payment arrangements and received an account number by mail. That would defeat the purpose of having a telephone order mechanism. It must be at least as easy to pay for merchandise or services via the Internet as is to place a credit card order by telephone. One must be able to do it without any prior relationship with the seller.

In other words, the Internet needs transaction-specific payment arrangements. Such payment systems can be based on credit card orders, or on newer forms of payment arrangements sometimes referred to as 'cybermoney', or 'cybercash'. For either type of payment system, public key encryption is promising. Public key encryption is a technology application that permits one to send secure messages and to authenticate the sender by means of two paired keys or codes, one possessed only by the sender, and the other available to anyone wishing to do business with the sender. Once the sender signs a message or payment order with his secret key, the identity of the sender can be verified with certainty because only that particular sender's public key will match the message. Someone wishing to send a confidential message to a person encodes it with that person's public key, and the message then can be decoded only by the addressee using her



secret key. Public key encryption is well understood and has been incorporated into a number of commercial products that are relatively easy to use and inexpensive on desktop computers and low-end Internet workstations.

Figure 7 shows the participants in a payment system implemented through public key encryption. The purchaser provides the seller with a payment order digitally signed with the purchaser's secret key. The payment order can be thought of either as a credit card payment order or the transfer of digital cash. The seller confirms the authenticity of the payment order by checking the digital signature with the purchaser's public key, a step shown in the diagram by the dotted lines running between the seller and the box labelled 'CA' (certificate authority). The certificate authority maintains a database associating public keys with a large number of persons wishing to do business with each other. The certificate authority database is like a specialized and very large white pages phone book, except that it vouches for the relationship between individuals and entities and their public keys, rather than vouching for the relationship between individuals and entities and their telephone number.

Having confirmed the authenticity of the purchaser's digitally signed payment order, the seller delivers the services or ships the merchandise, shown by the line at the bottom running from the seller to the purchaser. Then, the seller passes the payment order along to the issuer of the credit card or cybercash, and receives money or credit in return. Public key encryption also may be used to improve security of these last two steps in the financial transaction settlements process.

Thus described, the financial transactions are remarkably similar to conventional credit card transactions; indeed, the same figure could be used to explain conventional credit card transactions, with a credit card authorization center substituted for the CA, and the seller's bank substituted for the issuer, unless the same bank serves the seller and issues the credit card. The close resemblance between public key encryption-based Internet payment systems and conventional credit card transactions is a great advantage and hastens the deployment of good payment systems on the Internet, because existing institutions can, with relatively few changes, perform the necessary functions in the new systems.[4]

But attention also must be given to a legal infrastructure for the new payments. Most important, an appropriate legal framework must exist for certificate authorities. Legislation recently enacted by the Utah state legislature is an appropriate model.[5] It defines the responsibilities of certificate authorities so that purchasers and sellers of merchandise or services can rely on them to supply reliable public keys, and also clarifies the limits of liability for certificate authorities when things go wrong. This kind of legal clarification should permit entrepreneurial energies and market forces to develop an appropriate offering of certificate authority services.

It also is appropriate to give attention to the legal position of issuers of credit cards or cybercash. While it may be appropriate to adapt and extend banking regulation to such issuers because they really are playing a sort of banking role by issuing instruments that function as money, the experience of non-bank credit cards, such as American Express and Diner's Club Cards, and non-bank travellers' checks such as American Express and Thomas Cook travellers' checks, also suggest that the market and demonstrated reliability in redeeming obligations may function as well as legal regulation to assure customers of the integrity of issuers.

In any event it is appropriate to continue and accelerate the process already begun by UNCITRAL, Unidroit and the Uniform Commercial Code drafting committees to reformulate document based concepts in commercial law so that electronic commerce is not impeded by archaic legal requirements for the exchange of paper artefacts such as paper checks or paper credit card records of charge.

In the absence of these basic elements of legal infrastructure, the benefits of an open architecture like the Internet will be sacrificed because payment systems can be deployed only in closed proprietary systems in which payment is assured by conditions for membership in the proprietary network.

[4] Indeed, both Visa and MasterCard associations issued, in September, 1995, standards documents for secure credit card transactions on the Internet.

[5] Utah Digital Signatures Act, 1995 Utah Laws Ch. 61 (S.B. 82) (approved March 9, 1995), codified at Utah Code ß 46-3-101.

4 Can open networks be secure?

The Internet has a reputation for being insecure. The very features of the technology that permit its open, distributed, character – the routing and name and address database protocols – enable what Internet technologists call 'spoofing'. Spoofing involves the masquerading of one Internet host for another. Unless spoofing is prevented, forgery and undesired interception of Internet messages destroy requisite security. Current information on spoofing problems is available through the World Wide Web.[6]

In addressing open-network security, however, it is essential to focus on particular types of risk, and to adopt risk-based security measures. Three kinds of risks are involved with inadequate security: Invasion of personal privacy, as when confidential personal messages are intercepted and read or disclosed; compromise of commercial secrets or infringement of intellectual property; or, of particular interest to attorneys and physicians, compromise of professional secrets.

In addressing all three types of risk, it is important to be clear on the magnitude of the risk and to appraise security counter measures in proportion to the risk. It makes no sense to adopt a thousand pounds worth of security in order to protect against a twenty-five pence risk. Too often, the security dialogue is dominated by security specialists who insist that maximum security technologies be adopted even when the cost benefit of adopting sophisticated security technology is adverse. Often, relatively simple security measures such as appropriately managed user accounts and passwords are sufficient.

In any event, it is essential to focus as much on poor human practices and organizational procedures as on technological protections: 'who-based security' as contrasted with 'where-based security'. Good security depends on ensuring who participates in a transaction as much as where the transaction originates. Recent, highly-publicized Internet intrusions took advantage of trusted hosts – a where-based security protocol. An appropriate who-based security protocol would have prevented the intrusions. Passwords and user accounts are who-based. So are most digital signatures using public key encryption.

Two kinds of security improvements are now reality. A new Internet protocol – the basic IP protocol that determines how Internet packets are addressed and routed – now has been completed. IP v6 emphasizes secure routing and, can prevent spoofing.[7] Of course, before its benefits can be realized, it must actually be adopted, and adoption implicates all of the problems usually associated with gaining adoption of standards intended for broad use.

[6] at http://www.msen.com/'env/tubed/spoofing.html

[7] Information about Internet standards can be found on numerous sites including http://www.ips.id.ethz.ch/~parish/standard.html

The second security improvement is available from deployment of public key encryption at the application's layer, mass marketed software like Microsoft Windows 95 and Netscape. Until recently, law enforcement and national security concerns have interfered with such mass marketing of applications-level security because they have led to export controls that discouraged incorporation of good public key encryption features in mass marketed software. Now, however, the Clinton White House has announced greater flexibility in administration of export controls.

5 Improving the signal to noise ratio

The next question is whether intelligent systems can be used to improve the signal to noise ratio. When electrical engineers talk about the signal to noise ratio, they refer to how distinct the desired information is from background noise. Extending this idea to the Internet, one perceives higher signal to noise ratio when pertinent messages are not obscured by spam and random information not of interest to the particular user. Today's Internet has a number of applications intended to increase the signal to noise ratio. The World Wide Web itself assists users in focusing their attention and computing resources on material in a particular area, sparing them the necessity of downloading and reviewing much irrelevant material in order to find the desired items. Internet newsgroups and mailing lists perform a similar function with respect to interactive discussions. The signal to noise ratio issue thus overlaps concerns about improving search and retrieval precision and efficiency, and also overlaps ongoing efforts to define electronic communities more precisely.

Despite advances with Internet applications, any newsgroup user knows that much more remains to be done. In many active newsgroups, the garbage overwhelms the useful, and one must read many childish and – on occasion – pathological diatribes and irrelevancies in order to find the occasional intellectual gem. As the Internet becomes more democratic, more commercial, and more diverse, the problem is increasing. Regularly, for example, on specialized newsgroups set up to channel law student discussions on particular law school courses, as to which the feed is limited to participating law schools, postings pop up advertising a variety of activities and products and insulting the organizers of the groups. Many of these postings come from commercial services and there is no reason to believe that they come from law students or other intended participants.

The new technology does not reduce the long-standing need to organize various human activities to focus their attention on particular subjects. Just as much human energy is put into deciding whom to invite to a meeting and in chairing meetings effectively, so also does the Internet need human and technical tools to perform the same functions. Improved email screening and routing applications, and new combinations of newsgroup and list serve technology, such as the Villanova-developed 'LawGate', are incremental improvements, more of which are needed. LawGate links a newsgroup and a corresponding list so that a posting either to the newsgroup or the list shows up on the other, thereby permitting someone to participate in a discussion either by accessing the newsgroup through a newsreader or by subscribing to the list.

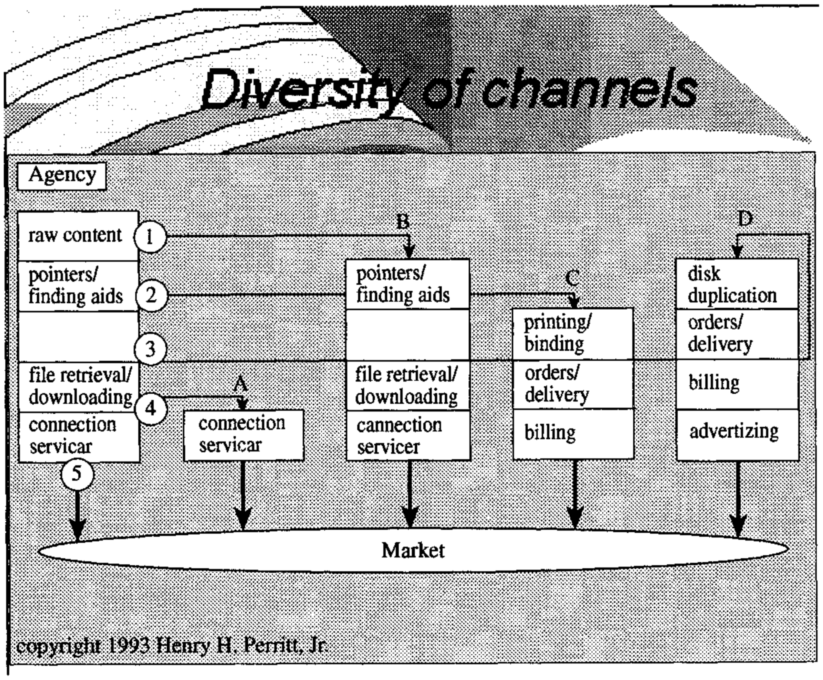
There will be no real electronic publishing unless users can find and retrieve desired information while masking everything else. Searching tools such as 'Lycos', the 'Web Crawler', the World Wide Web itself, the Z39.50 protocol and its associated Wide Area Information Service and better pattern matching using the tools of artificial intelligence, all are steps in the right direction to improve signal to noise ratios.

At the same time, however, it is appropriate to recognize that defining noise is not a trivial task. One person's noise is another person's valued speech. Democratic societies have been struggling for a couple of hundred years to strike appropriate balances between the need for freedom of expression on the one hand and the need not to be disturbed on the other. These freedom of expression balances need to be extended into the new technological environment, with appropriate attention to the differences made by the technology. In particular, the possibility of new bottlenecks blocking unpopular views from reaching the marketplace of ideas, new forms for the sword of the state censor, and new threats from private censorship by commercial intermediaries pandering to political extremists or to threats of lawsuits, all must be attended to if freedom of expression is to remain a reality in the new infrastructure.

6 Keeping public information public

Finally, public information must remain public. The information highway can go to Washington as well as Las Vegas; to Brussels as well as Cannes. But in order for this to happen, citizens and lawyers must remain vigilant to ensure that public information remains public. This assurance requires that copyright not be extended to government information, contrary to the British Crown copyright tradition; that statutory and common law rights to access public information similar to the U.S. Freedom of Information Act, be extended to electronic formats, and that public contracting policies not afford exclusive rights to distribute public information.

Recall Figure 1, and consider its application to government information. Sources of government information such as courts, legislatures, and agencies, shown in the circles above the solid line, can make their public information, including statutes, agency orders, and judicial decisions, available to their public simply by connecting computers on which the raw content is



maintained to the Internet. The agencies need not incur the costs of adding value added features or sophisticated, consumer-oriented telecommunication services.

A variety of value added redisseminators can facilitate public access to the information thus made available by connecting their own servers to the Internet, indicated by the triangles below the solid line. The costs of these entrepreneurs (which may be public or private) are reduced because they do not have to have the capital or the computing resources to maintain their own copies of the content. Instead, as the original description in Figure 1 explained, consumers combine the value added features to the content on demand.

There is, however, a wrinkle that potentially interferes with realization of the Internet's potential as an environment for wide dissemination of public information. Government entities confronted by budget pressures, as most are from time to time, realize that they can obtain revenue by offering value added information products. Many such agencies, working either directly or through contractors, put together a complete value added bundle, as shown on the left hand side of Figure 9, including not only raw content, but also pointers and user friendly interfaces, and communications services shown by rectangles in the value added bundle portrayed at the left hand side of the figure. Then, the agency realizes that it can enhance revenues by behaving as any monopolist, and eliminating access to its value added bundle except at point five at the price the agency sets. This excludes channels A, B, C, and D.

A, a provider of connection services only, would like to obtain access to the agency's information bundle at point four so that it could compete with the agency's connection services, but otherwise benefit from the taxpayer financed enhancements to the public information. Competitor B is perhaps most like WESTLAW and LEXIS. It would like to obtain access to the raw content at point 1, but wants to provide its own pointers and finding aids, presentation and user interfaces, file retrieval and downloading procedures, and connection services rather than paying the agency for its competing versions of these types of added value. Entrepreneur C is a conventional print publisher. It might want to obtain access to the agency information at point 2, taking advantage not only of the raw content but of some of the agency-established pointers and finding aids. Then, it wishes to provide its own added value in the form of printing and binding, order fulfillment and delivery, and billing, rather than having to pay for competing and duplicative agency-produced value items that correspond to these. Producer D is a CD-ROM publisher. It would like to obtain access to the agency's information stack and point 3, but to provide its own types of value as shown in Figure 9.

The diversity of sources and channels, now statutorily mandated in the United States by 44 U.S.C. ß 3506(d), added by the Paperwork Reduction Act of 1995, Pub.L. 104-13, 109 Stat 163 (May 22, 1995), ensures that the agency keeps open all these points of access, 1-4, as well as point 5, so that it does not maintain a monopoly on value added information bundles derived from its content. This diversity principle is reinforced also by the absence of copyright for agency-produced materials and the availability of access rights to any level of information value under Freedom of Information Acts.

7 Conclusion

Thus, the open network model for the global information infrastructure exemplified by the Internet can realize its potential, but only if appropriate attention is given to the development of payment systems, adequate security for personal and commercial privacy, further improvements in signal to noise ratio, and appropriate access to public information.

In addressing these issues, policymakers, lawyers, and academics from the European community and the countries of Europe have much to teach and much to learn, and so do policymakers, lawyers, and academics in the United States. Realizing the potential of the global information infrastructure really must be a transatlantic undertaking.