10th BILETA Conference
Electronic Communications

March 30th & March 31st, 1995
Business School, University of Strathclyde, Glasgow

Keynote Presentation

Henry H. Perrit Jr., Villanova University

Introduction

Legal automation has progressed beyond the boundaries of legal institutions. The basic work of convincing lawyers, judges, and law students that they can benefit from having desktop computers and from exchanging information across local area networks is done. A growing body of empirical data collected in the United States and elsewhere shows a remarkable rate of increase in the penetration of legal information technology in all branches of the profession. Five years ago it was eccentric to be conversant with such technology. Now, it is eccentric for a legal practitioner or law student to decline to use PC and LAN technology and legal databases.

It still is relatively unusual, however, for judges and practitioners to exchange information across the boundaries of their own institutions. A few clients insist on exchanging email with their lawyers and some institutional clients and law firms have set up electronic bulletin boards to exchange documents and notices. An even smaller number of firms file litigation documents with agencies and courts. Fewer than a dozen publish on the Internet. A somewhat larger proportion of the law student population regularly exchanges email with persons outside their law schools and participates in electronic discussion groups on the Internet or proprietary information services like America On Line and CompuServe. Most lawyers and law students, however, are perfectly content to use computer and digital communications technology almost entirely within the limits of their own institutions.

This is about to change. Because most people use information technology internally, most of the work product currently being generated by legal institutions exists in electronic form, presenting the obvious possibility that the costs of exchanging it with other legal institutions can be greatly reduced if information is exchanged electronically. At the same time, the Internet, considerably assisted by the Clinton Administration's National Information Infrastructure initiative, has seized the world's imagination. The Internet not only is inherently a concept that breaches organizational boundaries, it also is a realization of computer science concepts that greatly reduce the cost of wide area networking. Its nonproprietary standards, distributed information management philosophy, and its common name and address space substantially reduce the barriers to entry for information service providers, compared with the more traditional proprietary approaches represented by WESTLAW, LEXIS, CompuServe and America On Line.

The junction of electronic legal workproduct and the Internet represents the frontier of legal automation and computer law. This frontier should attract lawyers and others interested in the law: those interested in using technology to make legal institutions more efficient and fair as well as those interested in reengineering legal doctrine in light of changes in human behavior wrought by technology.

As on any frontier, however, there are major uncertainties about the patterns of development, about entrepreneurial opportunities, and about law and order. Of perhaps greatest importance to the legal community, there also are major questions about whether the frontier will remain available for appropriate exploitation by everyone in a competitive market environment or whether it will be parceled off into state monopolies before its potential is even explored -- whether Adam Smith's or Charles I's philosophy of governance will prevail.

The four major questions are whether an open, distributed, architecture like the Internet can be adapted successfully to provide economic incentives for production of information value; whether the same kind of technological architecture can adequately protect security, so as to prevent intrusions into personal privacy, compromises of commercially and professionally privileged information, and forgery and counterfeiting; whether database, pattern matching and rule based computer technology can reduce the noise to signal ratio to acceptable levels in a world wide distributed information infrastructure; and whether the legal profession can ensure that public information remains publicly available rather than being locked up behind technological and legal walls erected by state supported monopolies.

Incentives for Producing Information Value

The Internet is an incomplete model for broadly useful national and international information infrastructures because it does not yet offer payment mechanisms. Thus, electronic publishers and others who make their assets available to others through the Internet can have no expectation of being paid as others acquire those assets. This is beginning to change as commercial entities seek to exploit the potential of the Internet and to provide some value only to those who have made off line payment arrangements, or to persons making transaction-specific payment arrangements through credit cards or cyber money. Public key encryption is particularly promising as a technology for payment systems. It allows secure communications with a nearly unlimited number of trading partners by means of a combination of secret and public keys, both of which are used for each communication. Public key encryption also is attractive because it provides either secure digital signatures linked to message content, permitting a recipient to detect both forgery and alteration of contents; or privacy with respect to contents, or both.

Nevertheless, these payment systems are in their infancy. It is not clear whether they will be sufficiently convenient to attract purchasers or whether they will be sufficiently secure to reduce seller concerns about forgery, counterfeiting and dishonor of payment obligations. It also is not yet clear what legal infrastructure is necessary and appropriate for digital signatures based on public key encryption. (Most implementations of public key encryption require a publicly accessible database of public keys, usually called a "certificate authority," which vouches for the link between a particular public key and the owner.) The Utah legislature recently has enacted legislation to encourage and regulate certificate authorities, which is a useful model for other jurisdictions.

Of even greater significance than the form in which payment systems will prove effective is the inherent tension between the open architecture historically represented by the Internet and the practical need to limit access to particular products and services to those who have paid for them. It may be that as payment systems take root and mature on the Internet the result will look more like an interconnected WESTLAW, LEXIS, LEXIS Counsel Connect, CompuServe, and America On Line and less like the Internet of 1994. Even if that occurs, however, there may be enough left of the nonproprietary, distributed, and common name and address space characteristics of the Internet to make a commitment to the Internet architecture worthwhile.

In other words, there is a tension between open systems like the Internet and traditional ways of securing payment, which usually contemplate closed systems. But there also are major commercial advantages to open systems, which represent much larger markets than any single proprietary closed system ever can. Closed systems are like credit cards issued by and usable with individual department stores and gasoline companies. Open systems are like VISA and American Express. The challenge is to develop payment methods, probably using public key encryption, that work well in open systems like the Internet, offering convenience, security, and very low transaction costs.

It may seem that the need for payment arrangements is peripheral to the concerns of the legal profession, but this is not so. For one thing, good legal information will not be widely available to lawyers unless entrepreneurs can get paid for making it available. Thus, lawyers, as customers for appropriately organized statutes, case law, other primary sources and secondary materials will be disappointed unless the incentives are right for their sellers. Beyond that, lawyers are sellers of information. While it is not yet clear what form legal work product would take if it is exchanged on the Internet -- there are too many professional responsibility issues to be very certain about this kind of exchange yet-- it is conceivable that at least some lawyers in the future professional environment will provide legal advice and representation in exchange for relationships formed and carried out through the Internet. For this to work, there must be a way for the lawyers to get paid, and this requires payment systems.

Development and deployment of good payment systems requires that technology and law work together. Technology must address security and signature reliability; the law must allocate responsibility for security slip-ups and address the integrity of issuers of payment tokens. To do so, document-based concepts in commercial law like holders in due course and "negotiation" must be reformulated to fit paperless electronic commerce, as in the recently rewritten Article 8 of the UCC.

Security

The Internet has the reputation of being less secure than proprietary wide area networks. This perception is true at least to some extent, because there is no mechanism for excluding people from the network, and the same IP routing and name and address database protocols that make it relatively easy for a huge network to operate effectively as hosts are added or removed also make it easy for someone engaging in misconduct to pretend to be someone he is not (usually called "spoofing") and thereby obtain unauthorized access to resources. (The World Wide Web resources at http://www.msen.com/~emv/tubed/spoofing.html have very good information on the problem and solutions.) On the other hand, many of the routing and name and address service techniques that make the present Internet insecure are essential to any real infrastructure, access to which must be general. Thus, the same Internet characteristics that provoke so much security concern are the ones that make it an attractive model for the future. That means it is appropriate to understand the risks and develop appropriate protective measure rather than to reject the Internet as unsuitable and pursue proprietary network approaches instead.

There are three kinds of risks associated with insecure networks (beyond simple sabotage): the risk of invasion of personal privacy, the risk of compromising commercial secrets, and the risk of disclosing professionally privileged information. The personal privacy and commercial secret risks are of concern to lawyers as advisors and advocates. The risk to professionally privileged information is of concern to lawyers as professionals and as managers of their own practices. The legal implications of the three different kinds of security risks are different, but the technological sources of the risk, and the nature of appropriate countermeasures are the same for all three types of risk.

An essential part of any sound security strategy is to make the countermeasures commensurate with the risk. Much of the debate about computer security expresses concern over information that is essentially public in character and for which no significant expenditure for sophisticated security is justifiable. Other parts of the debate assume that expensive encryption and other security technologies are the only appropriate ways to protect against relatively modest levels of risk. In fact, almost all security has a cost, but some of the most effective security is inexpensive and focuses on the source of most security problems which is poor human practices and organizational procedures rather than defects in hardware or software.

The first line of defense for computer security is to have individual accounts associated with passwords, and a carefully thought out hierarchy of access privileges for different levels of capability. The best security strategy asks "who?" not "where?" The recent Internet intrusions took advantage of "trusted host" -- a "where?" -- security arrangement. "Who?" security is built into Novell's Netware, the dominant LAN technology, and also is built into UNIX, the foundation of the Internet. A recent article in the New York Times appropriately offered eight tips for safeguarding security in computer networks. Six of the eight steps involve password and account security rather than more sophisticated technological protection such as "firewalls." Nevertheless, it is certainly true that any slip up in security has larger risk implications the wider the set of computers in which one is connected. Mismanaging the password for access to one's own standalone computer gives rise to only trivial risks for most people, but mishandling passwords on a computer connected to the Internet potentially permits any wrongdoer in the world to get into that computer.

There are two kinds of improvements for computer network security visible on the horizon. One is the deployment of a secure Internet protocol, in which hosts authenticate themselves, thus making it much more difficult to spoof Internet addresses and thus circumvent firewalls. Another is the deployment of an encryption capability in the applications layer that will be usable world wide, adequately secure, and have acceptable performance. The first solution requires successful management of all of the problems usually associated with writing -- and gaining adoption of -- standards intended for broad use.

The second solution involves conflicts between security and privacy on the one hand, and the legitimate need of law enforcement and national security agencies to intercept criminal communications. This conflict energized the battle over the Clipper Chip recently fought more or less to a standoff in the United States.

It takes creative and flexible lawyers and political actors to work out encryption systems that are secure from inappropriate eavesdropping while also allowing access in appropriate cases. Developing and deploying appropriate security arrangements challenges legal institutions to adapt search warrant concepts and nondisclosure obligations to the realities of digital networks involving many intermediaries and much more-or-less anonymous communication. The systems and the legal concepts must operative effectively across national boundaries. They must deal with phenomena like "data havens" (storing data in a country where legal obligations are low in order to avoid obligations imposed in other countries) and "anonymous name servers" (Internet servers that permit a real person to hide behind an anonymous name).

Using Intelligent Systems to Improve Signal to Noise Ratio

Any regular user of the Internet knows that one of the most serious problems of universal computer networking is that the garbage tends to eclipse the useful. In most newsgroups within the Usenet community, for example, one must wade through scores or hundreds of irrelevant, bizarre, and verbose postings in order to discover a few nuggets of real timely value. Sometimes this is worthwhile because the nuggets are so valuable; other times the newsgroup has its own peculiar informal discipline that increases its signal to noise ratio. But as the Internet because more democratic, more commercial, and more diverse, the signal to noise ratio in most kinds electronic discussion areas and in much of the electronic publishing space will get worse. Even when some producers of information value impose intellectual discipline and good product quality control, their presence will be obscured by the crowd of others with lower standards. This means that the value of the Internet model as a base for discussion and for electronic publishing depends on the evolution of mechanisms to improve users' ability to find and retrieve the information useful to them while masking everything else. There is room to believe that this can be done.

The development of Archie in the late 1980s made it easier to find desired material on anonymous ftp servers. Gopher and World Wide Web are themselves techniques for identifying, and pointing to, subsets of information distributed across the Internet that may interest particular audiences. For example, the Villanova Law School web server (supported by NCAIR) specializes in identifying federal agencies that have Internet connections containing public information. The development of Veronica and Jughead free text search protocols help users find Gopher servers that may be of interest. The Z39.50 protocol and its proprietary implementation in Wide Area Information Service ("WAIS") allows full text searching to locate individual files published on a multiplicity of Internet servers. The Clinton Administration recently made a major commitment to Z39.50 in its Government Information Locator System ("GILS") initiative.

But much more needs to be done, ranging from the commercialization and successful marketing of robust programmable filters for email readers, to better newsgroup browsers, gateways between mailing lists and newsgroups which complement each other as virtual places for subject-specific discussion, with or without limited membership (Villanova's LawGatesm is an example), and more sophisticated pattern matching techniques to match a user desire against the characteristics of retrievable resources. This is where artificial intelligence may yet prove its utility in legal automation.

While most improvements in signal to noise ratio will come from better screens and filters, it also is true that one person's noise is another's valued speech. What Americans call First Amendment concepts -- more generally, freedom of expression law -- reflect balances struck over several centuries. These balances must be extended into a new communications environment in which the sword of the State and the commercial motives of the electronic newsstand operator may be equally threatening to a robust marketplace of ideas. Private censorship can cut off expression through new types private collaboration just as effectively as legal edict. The law must allocate responsibility for rulemaking, adjudicatory, and enforcement activities appropriately between public and private institutions. Articulating constitutional principles for governing cyberspace is an important undertaking.

Assuring that Public Information Remains Public

Information technology offers the potential for the entire citizenry of a state to obtain virtually immediate access to the documentary material of democracy and government under a rule of law. But the very technologies that make statutes, agency rules, judicial decisions, agency orders and land records readily available in national and international information infrastructures also create tempting economic incentives for their generators to set up monopolistic arrangements to generate revenue by restricting access. Because governmental holders of these types of public information have a natural monopoly on the content, they have the power to extend that monopoly into after markets for value added features. Typically, they accomplish this by asserting a de jure or de facto copyright over the material and weakening Freedom of Information Act public rights to access.

In the United States at the federal level, the current position is ideal. Copyright is unavailable by explicit statutory proviso (17 U.S.C. ' 105), and the Federal Freedom of Information Act (5 U.S.C. ' 552) is interpreted to grant unconditional rights to access basic legal information held by the executive branch. Similar constitutional doctrines are the source of similar rights to basic judicial and legislative information. The legal position of states and municipalities is less clear, mainly because they are not statutorily barred from asserting copyright, although the caselaw suggests the existence of Constitutional impediments to state and municipal copyright in basic legal information.

Britain and British commonwealth countries are at the opposite end of a spectrum on which are distributed most other developed nations. Copyright, coupled with the absence of anything like the Freedom of Information Act, means that Her Majesty's Stationary Office easily can generate revenue by restricting the activities of private redisseminators of public information, thus keeping prices high and blunting incentives to engage new technologies.

The legal community has a special responsibility -- to its clients, to the health of democratic political and legal institutions, and to its own practice activities -- to ensure that markets for public information remain competitive and vigorous. Only in this way can prices be low and the fruits of new technologies be dispersed quickly. Above all, public information policy must embrace the principle of a diversity of sources of channels for public information, and this best can be done by restricting copyright in public information and granting or ensuring the continuation of broad legally enforceable rights by both end users and publishers to obtain access to any existing format of public information, including the tools necessary for accessing it effectively.

This policy must also allow assertion of intellectual property in value added features so that private publishers have an incentive to disseminate public information. The challenge for public records and copyright law is nontrivial, especially when proprietary features are embedded in public information as frequently occurs with databases.

Conclusion

The Internet is a model of a worldwide information infrastructure that should enhance the functioning of democratic political systems and market economies. For the model to realize its potential, lawyers and law schools must help lawmakers solve four basic problems, regarding payment systems, security, usability, and access to public information. The agendas are abundant for those interested in the technology of legal automation and for those interested in the law of electronic networks. The evolution of new political institutions in Europe presents special opportunities to take advantage of new ideas.