The Internet rules of engagement: then and now

Leonard Kleinrock

Computer Science Department, University of California at Los Angeles, Los Angeles, CA 90095-1596, USA

Abstract

Imagine that we had carefully established the Rules of Engagement for the Internet in its earliest days around the time of its birth in 1969. What would those Rules have contained? What indeed, were the underlying principles and policies that we actually documented, said, understood, implied and instilled back then? What, if any, additional elements should have been included, given the benefit of the hindsight? How has the impact that the Internet has had upon society been influenced by the Rules of Engagement and in what ways do they need changing at this point? These are the issues of interest to this paper.

Keywords: Internet; Rules of Engagement; Guiding Principles; Internet Vision; Access; Regulation; Privacy; Internet Dark Side; Dispute Resolution; Spam; Malicious Behavior; Control.

1. Introduction

The Internet has been with us for almost 35 years now [1]. I have watched it evolve from its birth in 1969 to the juvenile, yet powerful force, to which it has now grown. In this paper, I wish to review the vision I had for the Internet back then and how I feel today about its successes, its failures, its surprises and its future.

To begin with, let's ask how well the Internet has done in realizing its early goals, vision, policies, and guiding principles? In so many ways it has worked wonderfully. The Internet has pervaded nearly all aspects of our lives as it leads us into a 21st century Information Society. It has fundamentally changed our institutions and business practices, our behavior, our attitudes, our social interactions our educational processes and our work habits. Nearly one billion people on this planet use the Internet today. Business is deeply and irrevocably dependent on it. The younger generation cannot conceive of a time when the Internet was not there to provide its many resources and capabilities. We can never turn the clock back to the pre-Internet world.

Why did it do so well? By design, accident, or luck, the Internet was able to tap into an enormous and universal desire when it made it possible for communities of people to communicate and interact quickly, inexpensively, easily and broadly. Earlier technologies such as the telephone, the postal system, the telegraph, the newspaper, the printing press, the television, etc, also made it possible for communities to interact, but they each suffered from one or more of the following shortcomings: only a few people could be reached at once; the interaction was slow; the interaction was one-way; the process was clumsy and cumbersome; or there was a large cost to interact with large numbers of people. The Internet changed all that and enabled rapid, essentially free, interactive, easy access to vast numbers of people. In fact, our first indication that human-to-human communication (as opposed to machine-to-machine communication) was an overwhelming attraction of the Internet was when email was first introduced to the Internet in 1972 [2]. Prior to that, there was relatively little traffic on the Internet. As soon as email was introduced, it generated large amounts of traffic and has dominated the Internet from that time forward. Ever since, whenever an application that enhanced the formation of communities of people has been introduced, it has been embraced quickly and effectively.

The secret of the Internet's power lies in the fact that it embraces and encourages hundreds of millions of people to contribute their creative ideas, knowledge and works and make them available to others interactively on the Internet. There is tremendous power in the Internet's philosophy of open research, shared ideas and works, no overbearing control structure, and trust in the members of the community.

However, there is a dark side to the Internet that has developed over the past decade. The dark side includes spam, invasion of privacy, pornography, pedophilia, denial of service, worms, viruses, destruction of property, and more. I address some of these below, but I wonder what it is about the Internet that has so seriously exacerbated this troublesome behavior. A partial answer lies in the fact that the Internet provides an enormous degree of anonymity to the perpetrators, far more than ever before possible. Moreover, the Internet allows one to reach hundreds of millions of users easily, quickly, and at essentially no cost (in money or effort). This combination of anonymous free pervasive access to others has helped to foster the dark side of the Internet. Earlier, I mentioned that older technologies failed to provide the broad appeal that the Internet offers, but at the same time the lack in each of those technologies also limited the extent to which the dark side emerged; to wit, neither the telephone nor the telegraph can simultaneously reach vast numbers of people, the postal system exacts a fee for mass mailings, the newspaper reaches many but has a cost associated with it and does not pester everyone who subscribes to the newspaper, the printing press is expensive, television reaches all but has a large cost for advertising and is still a one-way broadcast medium. The Internet removes these impediments to reaching millions of users and, as I said above, it does so with anonymity. This is the formula for enabling the dark side of the Internet.

I wonder if we could have done better back then in laying down a framework for proper Internet use and behavior. Frankly, in 1969 I was not especially worried about a dark side emerging in our benign and experimental network. We were focusing on the technical challenges of bringing about an incredible new technology whose benefits were very clear to me; who ever thought that we would reach a billion users, among whom would be malicious perpetrators of some really unscrupulous behavior[1]. Now I wonder what we can do to brighten up the dark side and soften its negative impact. Let us begin at the beginning – the early vision of the Internet.

[1] Let us not forget that some of the older technologies have developed some fairly dark sides which were not anticipated by their creators. For example, in the case of telephony, I doubt that Alexander Graham Bell ever imagined that his telephone network would be used for pornography, for unsolicited solicitations, etc.

2. The early vision

On October 29, 1969, the Internet came to life when it uttered its first words. On that date, the first message between two host computers was sent through the fledgling Internet from my laboratory at UCLA and received at SRI in Northern California [3]. We set up a message transmission to go from the UCLA SDS Sigma 7 Host computer to the SRI SDS 940 Host computer. The transmission itself was simply to "login" to SRI from UCLA. We succeeded in transmitting the "l" and the "o" and then the SRI host system crashed! Hence, the first message on the Internet was "Lo!", a most prescient message indeed.

A few months before that, on July 3, 1969, UCLA put out a Press Release [4] announcing the forthcoming birth of the Internet (known originally as the ARPANET [1]). In that document, I articulated my vision as to what the Internet would become. The opening sentence of that press release begins, "UCLA will become the first station in a nationwide computer network …". In the final paragraph of that press release, I am quoted as saying, "As of now, computer networks are still in their infancy. But as they grow up and become more sophisticated, we will probably see the spread of 'computer utilities' which, like present electric and telephone utilities, will service individual homes and offices across the country." The "computer utilities" comment foresaw the emergence of web-based IP services; the "electric and telephone utilities" comment foresaw the ability to plug in anywhere to an always on and "invisible" network; and the "individual homes and offices" comment predicted ubiquitous access by consumers as well as professionals. Basically, I had articulated a vision of what the Internet would become. (The part I did not include in my vision nearly 35 years ago was that my 96 year-old mother would be on the Internet today - and indeed, she is). That early vision for the Internet can be broken down into five elements:

1. The internet technology will be everywhere
2. It will be always accessible
3. It will be always on
4. Anyone will be able to plug in from any location with any device at any time
5. It will be invisible.

The first three elements have been achieved. With the advent of mobile nomadic computing, we are fast realizing the fourth element [5]. We have yet to achieve the fifth element.

But in fact, there was much more to the early vision of the Internet that we, the founders of the Internet, established as part of its original DNA. Most of this extended vision was not written into any documentation, but was an understood agreement among the parties involved. First, there was the deep commitment that there would be no centralized control authority. This concept of distributed control was inherent in the architectural design of the Internet. Indeed, in my early publications on the design of packet networks [6], I introduced a fully distributed routing control protocol that assured that no one part of the network had total responsibility for network control, but rather that all parts shared in that control. This was to become one of the fundamental tenets of the Internet design philosophy. A further manifestation of this principle was in the way the funding agency, the Advanced Research Projects Agency (ARPA) [7] managed the project; specifically, ARPA management allowed considerable freedom and flexibility in our research efforts, and they imposed a minimum requirement in terms of progress reports, meetings, site visits, oversight, etc, thereby not manifesting a strong centralized control of the network development. This enlightened approach was key in promoting the growth of the Internet. Indeed, ARPA made a "high-risk, high-payoff" bet, a bet that returned a handsome profit. As an extension of this tenet of shared control, we, the principal investigators, delegated the further development and implementation of the protocols and software to a distributed group of researchers and graduate students that self-organized themselves into a cooperating team [8], again with no central control. The net effect of this first unwritten agreement was that the control of the Internet was vested in all the people who were using the net, and not in the carriers, the providers or the corporate world. Second, the researchers and developers were driven by a strong sense of community in which the ideas and the products of our research were to be shared freely among all. That is, ours was an open network, open to new ideas, to access by all, to protocols and algorithms that were published and available, etc. Third, the gratification for us was not one of proprietary ownership, but rather the reward was the broad use of our creative works by others. As a result of this philosophy (as I said earlier), the net was an environment of open research, shared ideas and works, no overbearing control structure, and trust in the members of the community.

There were some additional basic concepts that were built into the network philosophy and design. One of these, the end-to-end philosophy [9], was that the intelligence of the network was best placed at the edge of the network, i.e., in its end devices such as intelligent terminals and computers. The job of the underlying network was simply to move data from one end to the other end without understanding or modifying the data it was transmitting. The idea was that the network would then be able to pass any kind of data the users chose to send instead of constraining the network to carry only certain kinds of traffic. A second element of the design came about because the community was trusted and cooperative, and so there was little emphasis put on protection against malicious user behavior in the architecture. Certainly there was considerable effort put into protection against errors, failures, and noise that might be generated from natural causes. But little effort was put forward to protect against nuisance, frivolous, mean-streaked or malicious attacks by the community itself. A third characteristic of the early Internet was the development of a sense of "Netiquette", the etiquette for cyberspace [10]. Netiquette developed as a shared sense of what constituted proper online behavior by the early users of email and other applications. One example that stands out is that one should not type an email in all capital letters since that gives the impression that one was shouting at the reader. The vast majority of users obeyed these unwritten rules in those early days; sadly, it is no longer so.

As a result of these early decisions, the Internet has had a long legacy of open access and use[2]. In the early days there was a limited membership of those who had access to the Internet. Having started as a resource sharing network[3] sponsored by the Department of Defense ARPA,

[2] I am often credited with making the first "illegal" use of the Internet, i.e., a personal use with no scientific purpose. The scene was a computer-communications conference held at the University of Sussex in Brighton, England in 1973 where we had set up temporary Internet connectivity for the conference. We were housed in the University's dormitories. I had to leave a day early, and, upon arriving home, discovered that I had left my electric razor in the dorm. I wanted it back. It was 3:00 am British time, and I wondered who would be wild enough to be on the net at that time of the morning. I concluded that my friend, Larry Roberts might well be and, sure enough, when I launched a network-wide query to find him, he was logged on to a machine in Cambridge, MA. I quickly set up a chat session with him, explained the problem, and the next day, my razor was delivered to me by my colleague, Danny Cohen.

[3] A widely held view is that the Internet was funded by the Department of Defense to create a network that would survive a nuclear attack. This view is false, an urban myth, which persists to this day. The true motivation for creating the Internet back then was, as I state above, to allow us to share resources across the net so that we could conduct research in computer science.

the use of the network was basically limited to those computer scientists in academia and industry who were funded by ARPA and to those in government who were involved in its use and development. This persisted into the 1980's. It was early in the 1980's that the National Science Foundation (NSF) [11] began funding a number of Supercomputer Centers around the United States. Later in the 1980's, NSF decided that these Supercomputer Centers needed higher speed connectivity than was available with the T1 links (1.5 megabit/sec) of the Internet at that time. So NSF upgraded the Internet backbone to T3 links (45 megabit/sec) and funded the resultant NSFNET backbone for the Internet. This had some interesting effects. First, it must be noted that NSF continued with the open access philosophy that had persisted for almost twenty years. Indeed, they articulated an especially liberal "acceptable use policy" [12] whose general principle was, "NSFNET Backbone services are provided to support open research and education in and among US research and instructional institutions, plus research arms of for-profit firms when engaged in open scholarly communication and research. Use for other purposes is not acceptable."

The effect of this policy was to allow access to the Internet for far more than just computer scientists. It provided access for all scientists (after all, this was the National Science Foundation) including, among others, physicists, chemists, biologists, geologists, astronomers, archeologists, oceanographers, etc. This greatly expanded the membership of users of the Internet. An interesting phenomenon occurred as a result, and this had to do the with .com organizations. Until the mid-1980's, most of the organizations that had access to the Internet were from the .edu, .gov and .mil groups. Once NSF admitted all manner of scientists, then the research laboratories of many commercial organizations (the .com companies) gained access. As reported earlier, email was a major application of great appeal and of course these research laboratories made heavy use of email as well as other useful network applications. It should have been obvious that once the other divisions of the .com organizations (e.g., management, sales, engineering, marketing, etc) saw how powerful these applications were, that they, too, would begin using them. And so it was that the .com organizations began to see the great power of the Internet and its applications. The Internet began to find its way well beyond the scientific community by the late 1980's.

A second development occurred around this time, namely, then-Senator Al Gore, a strong and knowledgeable proponent of the Internet, promoted legislation that resulted in President George Bush signing the High Performance Computing and Communication act of 1991. This Act allocated $600 million for high performance computing and for the creation of the National Research and Education Network [13-14]. The NREN brought together industry, academia and government in a joint effort to accelerate the development and deployment of gigabit/sec networking.

A third event occurred in 1993, namely, the creation of the World Wide Web [15] whose easy user interface and capabilities captured the imagination of the entire global community.

These three events (recognition by industry of the power of the Internet, gigabit/sec networking, and a powerful user-friendly interface to the net) launched the deep penetration of the Internet across the world and to hundreds of millions of users[4].

[4] One might imagine that the Internet has been "corrupted" by commercial use as opposed to the original idealistic vision of shared ideas and research objectives. I, for one, have no such concern. On the contrary, I believe that the rapid universal deployment of the Internet would not have occurred were it not for the energy provided by the commercial sector. The idealistic and

The stage was now set for the unbridled enthusiasm of the dot-com boom (and later bust) as well as the emergence of the dark side of the Internet.

The first significant sign of the dark side was spam. It surfaced as a critical and widely publicized event in April 1994 when two Arizona-based attorneys arguably became the two most hated individuals in the history of the Internet. It was Lawrence Canter and Martha Siegel, the famous "green card lawyers" who "spammed" the Internet. What they did was to post an advertisement for their immigration services (a U.S. "Green Card lottery" -- a chance for non-Americans to enter a very low-odds US-work-permit raffle) to almost every active bulletin board (the Usenet Newsgroups), thus ensuring that it would race across the Internet and be seen in approximately 140 countries by millions of users, not just once but over and over again. Though this commercial activity was not illegal, it came as a surprise to many users and violated an unwritten community code. The postings incited outrage in the newsgroup community and prompted tens of thousands of people globally to send hate mail and clog the in-box of Canter and Siegel's company. The onslaught of e-mail caused the company's Internet service provider to collapse, and Canter and Siegel were forced to sign on with another ISP. Thus, was ushered in what we all complain about today, spam.

3. Today’s realities and issues

The net has evolved into a powerful force in today’s society. As a result of the early Rules of Engagement that we created in a loose fashion we find in today’s world both good and bad characteristics on the net.

Among the good characteristics of the Internet, I include the following:

1. No one controls it
2. No one can turn it off
3. It serves everyone
4. In many ways, it is an “open” network
5. It provides a means to share works and ideas
6. It is diversifying
7. It is not centralizing
8. It is owned by no one
9. It is always turned on
10. It is empowering
11. It is a publishing machine
12. It offers a means of self expression
13. It is an innovation machine
14. It is a marketplace of ideas, services, applications, and goods
15. It connects communities of interest

In those early days, we quickly saw the power of communities of people interacting. But I certainly did not anticipate developments like the widespread popularity of buying and selling on the Internet (e.g., eBay).

Among the worrisome and dark-side characteristics of the Internet, I include the following:

1. It invades our privacy
2. It is capable of watching and tracking our behavior

commercial uses can live alongside each other as long as we protect the basic openness of the net.

3. It frustrates us with delays
4. It drowns us in junk
5. It does not obey the laws of all countries
6. It is a massive source of spam
7. It contains pornography
8. It spawns annoying and/or destructive viruses and worms
9. It supports denial of service attacks
10. It has developed into fences of proprietary products, services and information
11. Its user interfaces are frustrating

Let us group some of these dark-side characteristics into a few key categories and address the relevant issues.

3.1 Issues of access, regulation and censorship

Our early vision of the Internet was that of a cooperative shared infrastructure for all to access and use. We did not anticipate that special interests would place restrictions on who would be allowed access, and what could be transmitted. Today, we find ourselves dealing with those issues constantly and the fear is that hasty restrictions will be introduced that have long-lasting effects on an Internet which I see as hardly entering the stage of adolescent development. As an example, we have already seen the case of Yahoo signing off on content limitations in China which seems to open the door for portals to exercise censorship and content filtering in general [16]. An individual should be able to expect certain rights in the global society that we have created with the Internet. Perhaps self-regulation among agreeing parties will suffice to protect those rights, but we are seeing the case of national sovereignty taking precedence over international laws. Whatever the mechanism that emerges as the Internet evolves, a citizen should be able to access the latest information regarding the regulations that apply to his or her network use. Free information flow is in the interest of all nations and peoples. These issues apply to personal network use in the home, professional use in the workplace (i.e., employee/employer relationships), and citizen/state use.

Access to the Internet should not be denied to anyone and should only be curtailed in the case of proven abuse. Economic barriers to access must not be introduced; access to the Internet is the right of all people. The World Summit on the Information Society (WSIS) [17] has as one of its principal goals to find ways to provide the Internet revolution and its technology to the service of poor countries.

Moreover, the interests of commerce and business must not be allowed to dominate the ways in which the Internet is accessed and used. It must not be the case that the corporate world determines what content is allowed to pass over the Internet. It is important that we find ways to protect the openness that we designed into the Internet at its birth.

Freedom of expression and governance of the Internet are issues that are best addressed by top leaders in an international arena, with participation by all the stakeholders. To this end, the International Telecommunications Union (see below), a UN agency, has organized a UN conference, the World Summit on the Information Society (WSIS) mentioned above. For the first time, at the highest levels of government, there will be a global discussion of the challenges of the convergence between telecommunications, broadcasting multimedia and information and communication technologies. The anticipated outcome of the Summit is "to develop and foster a clear statement of political will and a concrete plan of action for achieving the goals of the Information Society, while fully reflecting all the different interests at stake". One of the tenets expressed by WSIS is that we must strike a fair balance between protection of intellectual property, on the one hand, and its use and knowledge sharing, on the other. This issue of balance is especially timely, given that the music industry has been engaged in a three-year legal war against peer-to-peer (P2P) networks for serving as conduits for alleged music piracy over the Internet [18]. Indeed, P2P networks have had a dramatic negative impact on the sale of music CD's and it is of concern that the same may happen to video sales. Here again, we did not anticipate this would occur with our open network, a network whose technology challenges enamored us at that time. The question arises whether we should have extended our original Rules of Engagement to address this issue back then.

3.2 Issue of privacy

We must insure that no individual's activities or data is tracked or monitored without that individual's knowledge. We have recently seen this privacy violated, to wit, in 2003 Jet Blue gave out information on millions of passenger itineraries and personal data to a Defense Department contractor to test the creation of a profiling system [19]. Another source of violation of this principle is in the license agreements that users of applications are forced to agree to before the application will run; these license agreements can be quite long, highly confusing, and often incorporate unreasonable terms of which the user is unaware. Location-based services also create a privacy problem in that individuals can be tracked without their being aware of it.

The technology must be designed to allow a user to specify what privacy policy he desires to have enabled.

Another concern involves children who are exposed to pornography, pedophilia, and other offensive material. There exists a Children's Bill of Rights for the Internet in which the overriding right is for a child "to feel safe and to be safe on the Internet" [20].

On Oct 2, 2003, the New York Times published a table [21] showing the sequence of nine US Federal Acts that Congress enacted that affect privacy. The first one listed was the 1968 Federal Wiretap Act which legalized wiretapping for federal law enforcement only if other investigative methods have been tried and are unlikely to succeed. It required a court order from a judge, finding probable cause for each crime being investigated. In 1984 the Cable Communications Policy Act restricted access to personal information about cable customers unless the customer was reasonably suspected of criminal activity, and the customer, upon being notified, could contest it in a court hearing. Following that, things went downhill for privacy (with the exception of the 1992 Cable Television Consumer Protection and Competition Act that extended the 1984 Cable Act to all other communication services (e.g. Internet access) offered over cable lines). By the time we got to the 1998 Digital Millennium Copyright Act (ISPs could gain access to personal information with no notification) and the 2001 Patriot Act (cable lines now subject to far less protection), it was clear that this sequence of privacy acts had vacillated considerably and the private individual had lost substantial protections of privacy. The concern with such a patchwork of federal acts is that these protections are not currently being preserved in a fashion that was intended when we first articulated the Internet Rules of Engagement.

End-to-end encryption offers some relief in this regard, and should be provided for and permitted; this would provide individual protection from governments and other entities from reading one's private communications.

The flip side of privacy is authentication. On the Internet, it becomes important that one be able to authenticate oneself. Given the fraud, spam, forged messages, etc, to which we are currently subjected, it is also necessary to be able to authenticate the provider and source of material that is delivered through the Internet.

3.3 Issue of dispute resolution

As founders of the Internet, we naively assumed that disputes would find ready resolution among the reasonable and well-meaning users of the early Internet. We assumed that an informal governance structure would suffice. In fact, that assumption worked well for decades. However, as the network has come to be populated with commercial organizations and other groups with their own vested interests, we have seen a clear divergence among the stakeholders regarding how the net should be governed, managed, and used.

There are at present a number of groups that address bits and pieces of these issues. Here I briefly identify and comment on some of the groups that currently exist and address the governance issue. I do so by listing the organization (in alphabetical order) and then abstracting from its charter or mission.

- **EFF**, the Electronic Frontier Foundation [22] is a donor-supported membership organization working to protect fundamental rights regardless of technology; to educate the press, policymakers and the general public about civil liberties issues related to technology; and to act as a defender of those liberties.
- **ETSI**, the European Telecommunications Standards Institute [23], is a not for profit organization whose mission is to produce telecommunications standards throughout Europe. ETSI represents administrations, network operators, manufacturers, service providers, research bodies and users.
- **ICANN**, the Internet Corporation for Assigned Names and Numbers [24] is the non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management.
- **IETF**, The Internet Engineering Task Force [25] is an open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
- **ISOC,** the Internet Society [26] is a professional membership society which addresses issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB).
- **ITU**, The International Telecommunications Union [27], is an international organization involved in standardization activities to coordinate the operation of telecommunication networks and services across the world.
- **NTIA**, The National Telecommunications and Information Administration [28], is an agency of the U.S. Department of Commerce that addresses domestic and international telecommunications and information technology issues.
- **W3C**, The World Wide Web Consortium [29] develops interoperable technologies (specifications, guidelines, software, and tools) involving the Web.

It is not clear if any of these organizations is fully representative of users, government, industry and academia in dispute resolution. They span a multidimensional space from a strong liberal view (EFF), to an engineering focus (IETF), to formal standards bodies at the international level (ITU). The creation of such a truly representative body for dispute resolution would be of great value and would enhance the proper and prudent development of the Internet as we move into the 21st century.

3.4 Issue of spam and other malicious acts

The fact that it costs the perpetrator almost nothing to send millions of email messages into the net is the principal cause of spam, viruses, worms and more. Indeed, the ability of the Internet to reach millions of people quickly, cheaply and easily is both a blessing and a curse. Everything gets amplified.

Legal means to stop spam (such as the current anti-spam law that is making its way through the US Congress [30]) are probably not effective, since we already have some pretty effective laws that impact some of the email one receives and it has not deterred its proliferation. In fact, using legal tools to stop spam quickly runs into issues of regulating dialogue and content on the Internet, including speech, and that is a slippery slope at best. Until we find a way to make the spammers suffer economic consequences, we will continue to have these excesses. I believe that the proper way to eliminate most spam is to introduce a charge to any site from which excessive email is being generated. This charge can also be used to slow down viruses by detecting when broad email storms are sent from a user (whose email traffic is being measured).

Another practice that eases the task of the virus writers, the spammers, and the attackers in general, is that the vast majority of users have adopted the same software application packages, and any flaw in that software can be exploited across hundreds of millions of machines. It becomes imperative that these widely used application packages be properly debugged and protected before they are released to vast numbers of users.

4. Recommendations to repair the things we missed

With the advantage of almost 35 years of hindsight, I offer the following list of some of the things we should have included in the original Rules of Engagement for the Internet. I recommend that we make these changes now. Most of them will be considered aggressive by some factions. Undoubtedly they will need some discussion before they will come to be realized.

- Access to the Internet should not be denied to anyone and should only be curtailed in the case of proven abuse.
- The interests of commerce and business should not be allowed to dominate or specify the ways in which the Internet is accessed and used. Neither should those interests control or regulate the content that passes over the Internet.
- An individual should be able to access the latest information regarding the regulations that apply to his or her network use.
- A user should be allowed to specify what privacy policy he or she desires to have enabled.
- No individual’s activities or data should be tracked or monitored without that individual’s knowledge.

- End-to-end encryption should be provided for and permitted, thereby preventing governments and other bodies from gaining access to one's private communications.
- The technology should allow for authentication of users, providers and all sources of network traffic.
- A charge for excessive email use should be considered as a defense against spam.
- A representative body for dispute resolution should be created and empowered.

Undoubtedly there are other Rules of Engagement that could be added. This is an ongoing discussion to which I hope I have contributed a good beginning.

5. Conclusion

The Internet has evolved dramatically since its birth in 1969. The Rules of Engagement with which it was endowed back then served it well for over two decades. The very success which has allowed the Internet to reach across the world and across our society so effectively has opened up the back door for the dark side to enter. Gone are the days when we could trust what came to us through the net, when we could expect that what was directed at us was relevant, useful, accurate and benign. Now we find ourselves confronted with junk, attacked by viruses, denied access, worried about our privacy, and confused about who can provide relief to these and other concerns.

What surprised me most is the extent to which the dark side has begun to cripple the Internet. Users are questioning whether they should continue to put up with the spam, the viruses, the updates, the worms, the invasion of privacy, etc. It is shocking how annoying and damaging these attacks have become. But we must not let that dark side justify the kind of controls that would cause the beneficial thrust of the Internet to diminish.

Now is the time to reevaluate the underlying assumptions of our original Rules of Engagement regarding how the Internet continues to be managed, adjudicated, cleansed and how it continues to grow. I fear that if we do not accept some of the recommendations I make in Section 4, then we will see a slowdown in Internet use and acceptance; if this happens, all of us lose. I realize that my recommendations may be viewed as controversial in that they advocate diminished influence by both government and industry. In defense of my position, we must take the long view and recognize that had government and industry attempted to influence the growth of the Internet in its early days, we would never have seen the Internet grow to its current prominence. Both government and industry benefited greatly from that relatively small investment by ARPA so many years ago. If we allow that influence to be felt now, I worry that we will stifle the Internet as we know it. Let us not kill the proverbial goose that laid the golden egg. We are proud of what the Internet has become, and if we take the proper steps now we will pave the way for its continued growth and promise. We must not ignore the lessons from the Internet history which taught us what it takes to succeed. Whatever we do or change, we must not stifle innovation and growth. It is essential that we maintain the basic concepts that were contained in the original philosophy of the Internet, namely, that it was founded on a heritage of openness and freedom, of open research, of shared ideas and works, with no overbearing control structure, and with trust in the members of the community. The challenge now is to balance that philosophy against the realities of today.

References

[1] Leiner, B., V. Cerf, D. Clark, R. Kahn, L. Kleinrock, D. Lynch, J. Postel, L. Roberts, S.Wolff, “A Brief History of the Internet”, *Communications of the ACM*, Vol. 40, No. 2, pp. 102-108, February 1997

[2] Tomlinson, R., “The First Network Email”, http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html

[3] Kleinrock, L., “The Day the Infant Internet Uttered its First Words”, http://www.lk.cs.ucla.edu/LK/Inet/1stmesg.html

[4] Tugend, T., “UCLA to be the First Station in Nationwide Computer Network”, *UCLA Press Release*, July 3, 1969, http://www.lk.cs.ucla.edu/LK/Bib/REPORT/press.html

[5] Kleinrock, L., “An Internet Vision: The Invisible Global Infrastructure”, *AdHoc Networks Journal*, Vol. 1, No. 1, pp. 3-11, July 2003

[6] Kleinrock, L., “Message Delay in Communication Nets with Storage”, *MIT PhD Dissertation*, December, 1962

[7] The Defense Advanced Research Projects Agency, http://www.darpa.mil

[8] The Request for Comments, http://www.rfc-editor.org

[9] Saltzer, J.H., Reed, D.P., and Clark, D.D., “End-to-End Argument in Systems Design”, *ACM Transactions in Computer Systems* **2**, **4**, November, 1984, pages 277-288

[10] [netiquette] Shea, V., “Netiquette”, Albion Books, http://www.albion.com/netiquette/book/index.html

[11] National Science Foundation, http://www.nsf.gov

[12] NSFNET Backbone Acceptable Use Policy, http://www.creighton.edu/nsfnet-aup.html

[13] National Research Network Review Committee, L. Kleinrock-Chair "Toward A National Research Network", *National Academy Press*, Washington, D.C., 1988.

[14] Nrenaissance Committee, L. Kleinrock-Chair, "Realizing the Information Future: The Internet and Beyond", *National Academy Press*, Washington, D.C., 1994.

[15] Berners-Lee, T., “Weaving the Web”, *Harper*, San Francisco, 1999

[16] Lemon, S., “Yahoo Criticized for Curtailing Freedom OnLine” PC World, August 12, 2002, http://www.pcworld.com/news/article/0,aid,103865,00.asp

[17] The World Summit on the Information Society, www.itu.int/wsis/basic/about.html

[18] Recording Industry Association of America, “Anti-Piracy”, 2003 www.riaa.com/issues/piracy/default.asp

[19] Foss, B. “JetBlue Gave Passenger Records to Defense Contractor” September 19, 2003, http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2003/09/19/national1505EDT0625.DTL

[20] Children’s Bill of Rights for the Internet, http://www.childnet-int.org/resources/billofrights.html

[21] Jehl, D. and Stout, D., “A Privacy Patchwork”, *New York Times*, page E7, October 2, 2003

[22] Electric Frontier Foundation, http://www.eff.org

[23] European Telecommunications Standards Institute, http://www.etsi.org/

[24] Internet Corporation for Assigned Names and Numbers, http://www.icann.org/general/abouticann.htm

[25] Internet Engineering Task Force, http://www.ietf.org

[26] Internet Society, www.isoc.org/isoc

[27] International Telecommunications Union, http://www.itu.int/home/index.html

[28] National Telecommunications and Information Administration, http://www.ntia.doc.gov/ntiahome/ntiafacts.htm

[29] World Wide Web Consortium, http://www.w3.org

[30] Spam Laws, http://www.spamlaws.com/federal/summ108.html

Leonard Kleinrock has served as a professor of computer science at the University of California, Los Angeles since 1963, serving as chairman of the department from 1991-1995. He received his M.S. and Ph.D. degrees from MIT in Electrical Engineering. Dr. Kleinrock is known as the Inventor of the Internet Technology, having created the basic principles of packet switching, the technology underpinning the Internet, while a graduate student at MIT. He was listed by the Los Angeles Times in 1999 as among the `50 People Who Most Influenced Business This Century'. He was first President and Co-founder of Linkabit Corporation. He is also Founder and Chairman of Nomadix, Inc., a high-tech firm located in Southern California as well as a Founder and Chairman of TTI/Vanguard, an advanced technology forum organization based in Santa Monica, California. He has published more than 225

Photo by Louis Bachrach

papers and authored six books on a wide array of subjects including packet switching networks, packet radio networks, local area networks, broadband networks, gigabit networks and nomadic computing. Dr. Kleinrock is a member of the National Academy of Engineering, a member of the American Academy of Arts and Sciences, an IEEE fellow, an ACM fellow and a founding member of the Computer Science and Telecommunications Board of the National Research Council. Among his many honors, he is the recipient of the C.C.N.Y. Townsend Harris Medal, the CCNY Electrical Engineering Award, the Marconi Award, the L.M. Ericsson Prize, the NAE Charles Stark Draper Prize, the Okawa Prize, the IEEE Internet Millennium Award, the UCLA Outstanding Teacher Award, the Lanchester Prize, the ACM SIGCOMM Award, the Sigma Xi Monie Ferst Award, the INFORMS Presidents Award, the IEEE Harry Goode Award.