Preface

Dale N. Hatfield*

I appreciate the opportunity to provide introductory remarks to this issue of *CommLaw Conspectus.* As unusual as it is to have a technologist do so, I believe it has become increasingly important for legal and engineering practitioners to become better acquainted with each other's fields of endeavor. This has never been so urgent as today, when we are confronted with a number of vexing issues related to the internet and the transition to the Digital Age, to which a number of articles in this issue of *CommLaw Conspectus* are devoted. Let me explain why.

In order to appreciate where we are going, we need to understand where we are today. As regards the internet, that means we must understand what makes the internet different from other networks. Stated differently, what accounts for the fabulous growth of the internet? If we don't fully understand what is producing the internet's success, how can we be sure that some public or private action—or lack of action—won't destroy whatever is producing its overwhelming success?

It is sometimes stated that the success of the internet lies in its reliance on packet switching. It is true that packet switching has a number of advantages over the traditional circuit switching of the public switched telephone network (PSTN). For example, in a packet network, users don't consume network transmission capacity when they are not generating information, which can be particularly beneficial when the information being transmitted is "bursty," as is often the case with data traffic. In addition, packet switching provides a degree of "bandwidth on demand" because, when more or less information needs to be transmitted, it is simply a matter of generating packets at a faster or a slower rate. Finally, different types of signals—voice, data, image, and even video—can be multiplexed together easily in a packet network, thus sharing transmission capacity and enabling multimedia applications to be developed.

Yet—if you will permit me to use a common legal expression—the packet switching response is "necessary but not sufficient." Packet switching has been around much longer than the recent ascent of the internet. I would argue that the success of the internet has more to do with the network architecture, and what that architecture reveals about the policy and philosophical choices that have been used to create the internet. What makes the internet different lies in the inter-related notions of (1) openness, (2) modularity and protocol layering and (3) the shifting of intelligence and control to the edge of the network. It is packet switching with a difference.

The internet employs an open architecture. Its standards and specifications are open, not closed or proprietary, and are freely available without any restrictions on use. The meetings at which the standards are set are also open. This emphasis on openness facilitates not only access by end users but also the interconnection of the private and public networks of which the internet is comprised. Further, the internet has been driven by people who believed that general consensus on a method or technique, and then developing the running code or functioning software, was the best sequence for moving forward. This contrasts with the sequence employed by more traditional government and telephone company standards bodies that first developed open paper standards and then tried to implement them in software, often paying a price in terms of complexity and delay. Finally, this sequence and the open architecture of the internet mean that the internet is

* Dale N. Hatfield is Chief of the Office of Engineering and Technology at the Federal Communications Commission. The views expressed in this preface are his own and may not necessarily reflect the views of the Commission.

more open to change and the development of new services and applications.

To understand modularity and protocol layering, it's best to begin by envisioning an hour glass, and to conceptualize the internet protocol at the waist of this hour glass. The network broadens above the waist to support a wide range of application and service layers such as e-mail and the World Wide Web, and broadens below the waist to enable those applications to ride on a wide range of underlying networks using a variety of technologies. This modularity and protocol layering promotes fair and open competition among multiple providers of the different layers. The resulting stratification—coupled with the openness described a moment ago—facilitates the introduction of new technologies and allows new applications to be devised and deployed, thereby stimulating innovation.

Innovation is also fostered by shifting intelligence and control to the edge of the network. Contrasted with the more centralized and tightly directed processes traditionally used in the PSTN, the routers in the internet perform what is basically a dumb function of forwarding data packets according to routing tables that are created on a largely decentralized, dynamic basis. In the internet architecture, control is shifted to increasingly powerful computers residing at the edge of the network. These computers are under the control of end users and service and content providers. This means that new services can be created without the cooperation or even knowledge of the underlying network provider.

Armed with an appreciation of what makes the internet different, we can better appreciate what may potentially threaten the continued success of the internet. These threats, as you may imagine, involve some of the very factors I have just described.

The first threat relates to layering and modularity. One of the fundamental strengths of the internet architecture is the separation of the application and service layers from the underlying network infrastructure, using the internet Protocol as the "glue" that holds them together. But separation does not necessarily imply that a provider shouldn't be able to compete at all layers. For example, there may be economies of scope in having a single firm provide multiple layers. Permitting providers to operate at multiple layers may produce additional incentives to construct facilities and to innovate more quickly.

The potential threat, however, comes when a provider has monopoly power in the provision of one layer—typically, but not always, the physical layer—and uses that monopoly power to discriminate in favor of its own services or content offered at the upper layers of the protocol stack. The discrimination can be in terms of the price charged for accessing the physical facility and/or the quality of the services offered by the lower layer to the higher layer. This threat is of particular concern in the subscriber access part of the network, where entrenched providers and some residual economies of scale may make competition at the physical layer problematic. Several contemporary policy and legal debates involve at their core these very concerns.

The second threat relates to interconnection. This threat stems from a number of different things. First, internet Service Providers (ISPs) are attempting to differentiate their networks through the provision of advanced features and functionality, such as quality of service (QoS) guarantees and Service Level Agreements. Clearly, such differentiation is a valued outcome of competition. Yet it tends to complicate both the technical and financial aspects of the interconnection or peering[1] arrangements among ISPs. Outright refusals to interconnect or failure to develop proper financial agreements to allow interconnection can lead to fragmentation of the network. Such fragmentation need not lead to a total loss of connectivity. However, available alternatives to peering, such as using transiting agreements,[2] may lead to inefficiencies and poorer performance—for example, in terms of latency or lost packets. Evidence of this fragmentation is indicated by the newspaper ads of large, backbone ISPs indicating the superior performance they

[1] Internet backbone providers interconnect for the purpose of exchanging each other's traffic. One form of interconnection agreement, known as peering arrangements, provide for the exchange of internet traffic for free, that is, without the payment of settlement charges. Typically, peering arrangements are used when the amount of traffic flowing in each direction is roughly equivalent.

[2] Transit arrangements are another form of interconnection agreement, involving payments from one provider to the other. They are typically used when the amount of traffic is unbalanced.

can provide if traffic stays on their network from end to end.

The third threat relates to a host of developments that are associated with trying to improve the performance of the internet. These improvements include steps to improve the security, manageability, and scalability of the internet and to offer better reliability and more predictable performance in terms of packet loss and latency or delay. The concern here does not stem from the objectives behind these improvements. They are laudable. Instead, the concern stems from the fact that the remedies may result in a return to a more centralized form of control.

For example, techniques for providing greater manageability and improved QoS may involve deciding on a particular route to follow and reserving end-to-end capacity on the network at the beginning of the session or call. This represents a more connection-oriented, arguably more centralized approach to networking. It is a departure from the decentralized, connectionless, best-effort network approach used in the internet in the past. This may not necessarily be bad, but carried out improperly or carried to an extreme, it could shift intelligence and control back to the center of the network in such a way that it undermines one of the major advantages of the traditional internet architecture. That advantage, as discussed earlier, is the ability for entrepreneurs to quickly create new services using the intelligence and control residing at the edge of the network, and to do so without the cooperation or even the knowledge of the underlying network provider.

The latter point leads me to a broader thought—the relationship between the internet and the public switched telephone network. The sheer magnitude of the investment in the traditional PSTN means that it will be around for many years. This creates the obvious need for backward compatibility between the internet and the PSTN. The internet and the PSTN will have to come together in some way, if for no other reason than to create efficient forms of interconnection and interworking. This process of coming together is just beginning, and a key question is how to meld together these two different worlds—the more decentralized, open world of the internet and the more centralized, closed world of the PSTN. How do we do so while maintaining the strengths of each?

Let me conclude by stating that while I have identified some potential threats to the continued success of the internet, I do not necessarily want to leave the impression that government action is needed to try to prevent or forestall them. Clearly, government action should be the last resort. In fact, I raise these potential threats in the fervent hope that the open, voluntary governance of the internet coupled with competitive, marketplace forces will be more than sufficient to protect it against them.

One need only look at the range of issues covered in this issue of *CommLaw Conspectus* to know that it makes an important contribution to the dialogue about how best to ensure the internet's continued success. Thank you for the privilege of letting me be a part of this dialogue. I hope that, by adding some important technical considerations, I have enriched the discussion of this critical issue.