

The Internet at

By James X. Dempsey

RISK

The
Need for
Higher
Education
ADVOCACY

The higher education community has long appreciated the potential of the Internet to expand access to information, facilitate communication, and promote human development. From the inception of the Internet, colleges and universities have worked to advance the realization of that potential. Today, advocacy in support of the open, innovative, and user-controlled Internet is more important than ever. The Internet has not grown by accident, nor is its future ensured. In fact, a number of current policy trends and pending proposals could radically change the nature of the Internet.

James X. Dempsey is Policy Director for the Center for Democracy and Technology (CDT).



The Internet was never a Wild West frontier, free of legal controls, that now, suddenly, in its mature state, requires policy intervention.

The Internet has benefited from a policy framework well suited to its unique characteristics. It is important that those engaged in Internet policy advocacy understand the technical and architectural features that make today's Internet uniquely powerful. Sound policies will reinforce those features; policies that are inconsistent with those features must be viewed skeptically.

If one looks at today's Internet and compares it with other media, certain qualities stand out:

- To a much greater degree than any other medium that came before it, the Internet is open and decentralized. It has few gatekeepers. Functionality is intentionally pushed to the edges

of the network, where innovative applications can be offered without the permission of network operators.

- The Internet offers a high degree of equality. Any item of data is as accessible as any other item of data, and all points on the network are equally accessible from every other point.
- The Internet is inexpensive. It poses relatively low barriers to entry: a computer and an Internet connection are far less expensive than a printing press or a radio station or the kinds of distribution networks that were traditionally required to reach large audiences.
- The Internet is abundant. Traditionally, radio and television technology was bound by the limited technical capability to exploit the electro-



magnetic spectrum. There was, and to some extent there still is, a scarcity of spectrum; consequently, government regulation of the airwaves was deemed necessary to allocate that scarce resource. The Internet, by contrast, can accommodate an essentially unlimited number of points of entry and an essentially unlimited number of speakers.

- The Internet is global and borderless. The fact that the Internet is less susceptible to some forms of geographically based regulation has legal ramifications. For example, the United Nations' Universal Declaration of Human Rights speaks about the right to receive and impart information regardless of frontiers. That 1948 language should be especially potent in the Internet age.
- The Internet is user-controlled to a far greater degree than other media. Internet users have the power to choose where they will go online and what they will see or hear. Users can configure their browsers and control their search engine results to avoid content they consider objectionable. Parents, teachers in elementary schools, and others in caregiver contexts can install filters to block unwanted content. Assuming that users are provided with notice and genuine choices, they can control what software is downloaded onto their computers. They can install security software at the desktop level to protect against many forms of fraudulent behavior. And now, of course,

user-generated content is changing the Internet, further empowering users.

- The Internet is uniquely versatile, making it especially suited to innovation. Vint Cerf, one of the fathers of the Internet, is fond of talking about “IP on everything and everything on IP,” by which he means that the brilliance of the Internet Protocol and associated standards is that they can operate over any medium—including the copper wire of the traditional telephone network, the coaxial cable of the cable network, the airwaves, and even power lines—while at the same time every form of content (voice, data, and video) can be carried on IP.

These unique technical and architectural characteristics have produced a technology of freedom and innovation. In only about two decades, the Internet has become a powerful global platform offering unprecedented access to information and supporting the formation of communities and the exchange of ideas

internationally. It has yielded a revolution in education, it is a powerful tool for democratization, and it offers significant improvements in the quality of health care, among other services.

How did we get here? Contrary to common (mis)perception, this open, innovative, user-controlled Internet did not arise in a policy vacuum. The Internet was never a Wild West frontier, free of legal controls, that now, suddenly, in its mature state, requires policy intervention. The fact is that from the beginning, the Internet has been enabled by a policy framework suited to its unique qualities. That legal framework has emphasized openness, competition, innovation, trust, consumer choice, and freedom of expression.

For example, whereas Internet Service providers (ISPs) themselves have always been relatively unregulated, they benefited from the open platform of the telecommunications infrastructure, which in the United States was based on the competition-enhancing principles of interconnection and nondiscrimination.

Under the regulatory principle of interconnection, every provider of telephone service had to interconnect with every other provider. No dominant carrier could say to a competitor or to another carrier, “We will not carry your content,” or “We will not interconnect with your network.” And under the principle of nondiscrimination, a telephone company could not charge higher rates to its competitor than it charged, for example, to its affiliated ISP, and it could not favor the traffic of one content provider over the content of another.

Another regulatory action that provided part of the legal underpinning of the Internet was the 1968 *Carterfone* decision, in which the Federal Communications Commission (FCC) ruled that AT&T could not prohibit its customers from attaching, to the edge of the telephone network, equipment that was not made or approved by “Ma Bell.” The device at issue in *Carterfone* was an odd invention that connected a two-way mobile radio system to the telephone network. The FCC ruled

that AT&T had to permit its customers to use any equipment so long as it did not cause damage to the network. This decision proved highly beneficial to the Internet, because when it became apparent that the analog network could be used to carry digital content, telephone network operators were required to allow their customers to connect modems to the network, and soon a remarkable amount of innovation was occurring at the edges of the network.

Another crucial policy choice was made in 1997 when the U.S. Supreme Court, in *Reno v. ACLU*, accorded the Internet the highest form of First Amendment protection. The Center for Democracy and Technology (CDT) played a key role in that landmark case. At the time, there was debate about the correct legal category for the Internet. Congress had passed a law restricting the transmission of explicit materials via the Internet—implementing restrictions similar to those that applied

to broadcast television. When the law was challenged before a panel of three federal judges in Philadelphia, CDT brought the Internet into the courtroom, to computers right on the dais where the judges were sitting, and offered a tutorial showing how the architecture of this technology was completely different from the architecture of radio and television networks. Citing the unique user-controlled nature of the Internet, that judicial panel and later the Supreme Court ruled that the Internet was entitled to the highest level of free-expression protection.

Another crucial set of Internet policies revolves around the issue of trust. To use the Internet for commerce and interpersonal communication requires a degree of confidence in its privacy and security. Even before the Internet became widely available, Jerry Berman, the founder of CDT, organized the Digital Privacy and Security Working Group, which brought together software and hardware manufacturers, ISPs, cellular carriers, traditional telephone companies, and others to press for privacy protections for all forms of electronic communications. Congress responded by enacting the Electronic Communications Privacy Act (ECPA) of 1986. ECPA updated the laws on government surveillance, establishing the principle that e-mail in transit would have the same legal protection traditionally accorded to telephone calls. Thus, if the government is seeking to intercept the content of any form of electronic communication, ECPA requires a court order based on the constitutional standard of probable cause. ECPA also requires the government to get a court order, albeit one based on a standard that now seems too low, to collect the transactional data associated with both telephone calls and Internet communications.

Another conscious policy choice that proved crucial to the development of the Internet was the decision not to regulate its technical design. Even though the Internet was born under the auspices of the Pentagon, the U.S. government never mandated its core technologies. Instead, the technology of the Internet has been largely left to voluntary, consensus-based standards bodies such as the Internet Engineering Task Force. The debate over controls on



This protection from liability has been a crucial element of the policy framework that has allowed the Internet to flourish.

has been legally reflected in the congressional policy that service providers are not liable for the content created by their customers. This protection from liability has been a crucial element of the policy framework that has allowed the Internet to flourish. If ISPs, Web hosts, and Web site operators become liable for content posted by others, the Internet will be stifled by gatekeepers and will cease to be a medium in which everyone has an equal voice.

The policy choice to protect intermediaries from liability not only has allowed service providers to expand rapidly but also has reinforced the principle of user control. Research has consistently confirmed that the best way to protect children from inappropriate content is through user education and user-controlled tools such as filtering software,

chosen by parents and teachers. Recently, however, policymakers are proposing to require ISPs to filter undesirable content. Congress also has increasingly considered delegating enforcement obligations to other intermediaries in online commerce, particularly credit card companies, forcing them to block payments to certain undesirable services. Most recently, as social networking sites have generated fears about children's safety and the exposure of children to inappropriate content, policymakers have threatened to impose obligations on the hosts of social networking sites.

These proposals violate the proven principle of user control. Instead, Congress should be supporting ways to empower users, for example by encouraging efforts to educate parents on the use of technology tools to shield children from

encryption is one example of this principle (and the principle of user control) at work. In the 1980s and 1990s, the government did initially regulate encryption technology, but ultimately policymakers concluded that the security interests of both Internet users and the government would be better served if the government did not try to regulate encryption but rather allowed a market to develop to serve the security needs of government, corporate, and individual users.

Within this patchwork of regulation, nonregulation, and self-regulation, it is possible to discern some overarching themes—ones that should guide policy in the coming years. At least four unifying principles define the successful policy framework that enabled the Internet to grow as remarkably as it has over the past two or three decades: (1) user control, (2) innovation, (3) trust, and (4) the dual values of openness and competition. These principles should guide legislators, advocates, and users in sorting through current policy proposals: Will the proposal increase or diminish user control? Will it promote or stifle innovation? Will it enhance or undermine trust? Will it keep the network open and foster competition, or will it impose gatekeepers and impede competition?

Members of Congress seem to be unaware of the value of *user control* as they offer a number of policy proposals that would address concerns about undesirable content online by requiring service providers to act as police. To date, the Internet's architectural lack of gatekeepers



A middle ground must be found that protects intellectual property while permitting and promoting innovation.

inappropriate content. Policymakers should also be focusing on programs that will teach children about the risks they face in online communities, such as some social networking sites. Experts on social networking and children at risk have shown that the children who are getting into trouble online are already at risk and that they are doing things online

that they are also doing in the real world, such as meeting adults they shouldn't be meeting. Of course, we all want to protect children against online abuse. But policymakers and all of us—as parents, educators, and people who care about children and the Internet—should focus our efforts on protecting and supporting at-risk children in both the online and the offline worlds, rather than demonizing the online environment. We need to educate children, just as we always have in the offline world, about what is appropriate and inappropriate behavior, so that they know what is right and what is wrong in terms of an adult approaching them and trying to get close to them. Although there are certainly risks online, the breadth of information that the Internet makes available to young people pro-

vides them incalculable benefits, and we should be teaching children to reap those benefits while staying safe online.

Innovation is another value at stake in current Internet policy debates. Government control over technology is fundamentally incompatible with innovation, yet some policy proposals under consideration in recent years would impose technology mandates. Intellectual property is one area where design mandates have been proposed. The digital age, of course, poses both opportunities and challenges for the creators and owners of intellectual property. A middle ground must be found that protects intellectual property while permitting and promoting innovation, fair use, and the ability of digital technology to facilitate free expression. However, one of the proposals that

have been put forward in the name of defending intellectual property is the technology mandate known as the “broadcast flag.” The broadcast flag was initially imposed by the FCC and would have required every device capable of handling digital video content to have a built-in government-approved technology that would read and respond to a “flag” marking television programs as copyrighted, thus limiting how the programs could be copied and shared. A federal court struck down this mandate, holding that the FCC lacks statutory jurisdiction to impose such a regime on a broad range of computing and electronics devices. But the notion of requiring device manufacturers to seek FCC approval for the design of the anti-piracy features of their devices continues to have its supporters.

Another technology mandate that has now gone into effect involves making the Internet easier to wiretap. In 2005, the FCC held that broadband Internet access and “interconnected” voice-over-IP (VoIP) services were subject to the design

standards of the 1994 Communications Assistance for Law Enforcement Act (CALEA). CALEA requires telecommunications carriers to design their switches to be wiretap-friendly. When it enacted CALEA, Congress concluded that such a requirement was appropriate for the centralized and relatively highly regulated public-switched telephone network but not for the decentralized and rapidly changing Internet. Therefore, when Congress passed CALEA, it explicitly specified that the law would not cover “information services,” which was regulatory shorthand for “the Internet.”

In most contexts, the FCC has allowed VoIP to proceed as an unregulated service, and for most purposes, the FCC has ruled that broadband Internet access is an information service exempt from regulation. However, the FCC completely reversed itself for purposes of CALEA and held that broadband Internet access and VoIP were subject to the requirements of CALEA, with yet-undetermined consequences for innovation. The FCC

discounted the fact that Internet services were already capable of being intercepted. Indeed, in many ways the digital revolution has been a boon for law enforcement, since the technologies on which we all depend generate more and more information about our activities on a daily basis—information that is often readily accessible to the government, often under weak privacy standards. Despite these trends, the government wants to put its thumb on the scale of technology development and push the technology in a way that further enhances the surveillance potential of the technology, without regard to the impact on innovation.

The FCC’s CALEA decision also implicates another one of the key defining principles underpinning the success of the Internet: *trust*. Congress and the states have sought to promote this trust with laws protecting the privacy and security of communications and of information collected and stored online. The premise of ECPA was that this technology would flourish only if users were assured that

Long-standing concerns about online privacy have been exacerbated by recent mergers of major online services companies.

their online communications were protected. Congress determined that an e-mail in transit should have essentially the same protection as a telephone call or a letter. Therefore, ECPA provides that communications are protected against government surveillance without a court

order, based on meeting the high “probable cause” standard of the U.S. Constitution’s Fourth Amendment.

This trust is at risk. Those who offer Internet access and online services, including institutions such as colleges and universities, are sitting on a growing body



of personally identifiable information about their users. The depth and breadth of the information that is generated about people’s daily lives and that is stored online goes far beyond anything anticipated in 1986, when ECPA was enacted. The current crazy quilt of privacy laws and judicial decisions is no longer sufficient to protect that information. The government, for example, argues that it is able to intercept location information from cell phones under a very low standard. Congress further weakened some of the standards for government surveillance in the PATRIOT Act, and in August 2007 it adopted legislation allowing for warrantless interception of international communications. Rather than weakening the standards, policymakers should be strengthening them, authorizing government access when needed but only pursuant to checks and balances suited to the intrusive potential of this technology.

Trust also requires baseline privacy and security rules for commercial data collection and use. Long-standing concerns about online privacy have been exacerbated by recent mergers of major online services companies, potentially bringing together larger stores of data for use in “behavioral profiling.” The information technology revolution in health care offers huge benefits but also makes health data more liquid, placing it at greater risk of unwarranted disclosure. At the same time, major technology changes are under way in the creation and management of identity: we are approaching a world in which almost everything,



Regulation need not cover the entire broadband network or prevent experiments with new architectures or business models.

the consumer privacy issue soon, but finding consensus will not be easy and will require the conscientious engagement of a wide range of stakeholders.

The debate over “Internet neutrality” implicates the dual principles of *openness* and *competition*. The narrowband, dial-up Internet was an open platform, offering equal treatment to all users and all content providers. Legal and marketplace changes associated with the transition to broadband have placed that openness at risk as network operators have gained the legal freedom to favor some content, services, or applications over others and have expressed interest in doing so. Although the principles of user control and innovation weigh against regulation when users have sufficient choices and information, the

including all actions online and off, will be personally identifiable. There simply is no policy framework for this environment: who collects information about us, with whom is it shared, what purposes can it be used for, and what control will we have over it? There is some expectation that Congress will seriously take up

concentrated nature of today’s broadband market may make this an instance in which regulation is needed to guard against the rise of new gatekeepers and to preserve the open nature of the Internet.

To be clear: regulation need not cover the entire broadband network or prevent experiments with new architectures or business models. Rather, regulation should focus on the targeted goal of ensuring that a portion of the converged broadband network remains open to all content and applications on a nondiscriminatory basis. Preserving this “plain vanilla” Internet, perhaps alongside other offerings, would serve the principles of user control and innovation by enabling Internet users to access any content of their choice and by allowing innovators to reach any users, all without technical interference or discrimination by the network operator.

Obviously, the four principles that should guide Internet policy—user control, innovation, trust, and openness/competition—are not exclusive or dispositive. The United States needs to fight terrorism. There is a strong interest in protecting children online. Intellectual property is a cornerstone of the U.S. economic system, and the copyright laws are in part intended to promote innovation. So the challenge we face going forward is to develop an Internet policy framework that addresses these clear needs while at the same time promoting the innovation and other values that have fostered the growth of this amazing medium. The higher education community, which hosted many of the wizards who created the Internet and which has woven this technology into every aspect of education, has a responsibility to work to defend the policy framework based on user control, innovation, trust, and openness/competition—so that the Internet in years to come is able to reach its potential as an empowering platform for learning, democracy, commerce, and human development. *e*