

> THE SPEED LIMIT ON THE INFO HIGHWAY RISES > INTERNET NAME REGISTRATION GOES GLOBAL > UNITED STATES LIFTS CONSTRAINTS ON ENCRYPTION EXPORTS > THE RANKS OF THE DIGITAL ECONOMY GET CROWDED

■ The Internet

RICHARD
COMERFORD
Senior Editor

IN DEVELOPED NATIONS AROUND THE WORLD LAST YEAR, the Internet entered the mainstream of consciousness. This year, it enters the mainstream of daily life. Improvements in speed, accessibility, and usefulness—coupled with the lowest prices ever for computers and free Internet access, or vice versa—will likely make for the most explosive growth yet. And business is expecting to make the most of that growth. The only obstacle to global progress is regulation...and the need to make the Internet robust enough to stand the traffic.

INTO HIGH GEAR

In 1999, phone and cable companies in North America, Europe, and other industrialized regions put into place the technologies needed to dramatically boost Internet access speeds—that is, digital subscriber loop (DSL), cable modems, and satellite links—and started hooking people up en masse. These new connections are transforming the Internet experience. For one thing, they do away with the so-called World Wide Wait, now that Web pages can stream in over 100 times faster than with 56-kb/s modems [Table 1]. For another, they put everyone on-line whenever they fire up their systems, letting e-mail come in and go out as easily as phone calls. And it is a good thing that the speed is increasing, because new developments at the World Wide Web Consortium, Cambridge, Mass., are going to require more data and make the Web more appealing. The consortium is changing the look and feel of the Web, enriching it both sensually and in terms of data usage.

The change embodies two new recommendations, as the consortium terms standards: the extended hypertext markup language and the synchronized multimedia integration language (XHTML and SMIL, respectively). Together, they alter how Web documents are created, in the process making it much easier to use more content, or data, in each Web page.

XHTML goes on from where earlier versions of the HTML language, more especially HTML 4.0, left off. It completely overhauls HTML to make it compatible with the extensible markup language (XML), a simplified version of the standard graphics markup language (SGML). The result of all this work is that XHTML users will find it easy to specify the precise look of a Web page (which is what SGML did for electronic documents, but in a very complex way). Pictures will appear where they should, not on top of text, and text will have the kind of font, leading, and justification the designer wants. So designers will be free to use more graphics and assorted fonts.

SMIL was released as version 1.0 in 1998, but was hard to use. So a new version is being readied for release in mid-year. Once deployed, the new version will let designers easily enrich pages with multimedia and, like XHTML, will give them more control of a Web page's appearance. Suppose the goal is a Web page in which an animation sequentially brings up pictures of popular 1950s children's heroes: The Lone Ranger, Superman, Batman, and so on. As each appears, the designer would like the hero's theme music to play (*The William Tell Overture*, for instance, would accompany the picture of The Lone Ranger). Today, the designer would have to attempt the well-nigh impossible—add just enough dead air to the start of the audio file to give the animation time to download. Of course, since download times vary widely, the designer would have to be omniscient to know how much dead air to add.

SMIL instead lets the designer simply state that the audio should begin at the same time as the animation [Fig. 1]; an SMIL-compatible browser—Netscape and Microsoft both support the standard—takes over from there. Existing multimedia formats, like the musical instrument digital interface (MIDI) and audio-video interleave (AVI), can be used.

The two new standards are likely to result in much more active and changing Web pages, with lots of animation and sound. Given those capabilities, the world of Web design will have to mature really quickly. Amateurish use of the standards will drive viewers to distraction, turning them off and away. But not using the new tools will soon yield distinctly monotonous pages. So the demands of e-commerce for increased sales will soon separate the wheat from the chaff.

NET IMPROVEMENT

The technology underlying the Web must also change if it is to keep up with demand. For one thing, the 32-bit Internet Protocol (IP) addresses specified by IP version 4 will soon be exhausted; already they are in short supply. The only cure will be to roll out the next version of the protocol, IPv6, with its 128-bit address space. While the new standard has been ready for some time, there has been little need for it. So network administrators have deferred the switch to software that supports it, which in turn prevents use of the longer numerical addresses. But the boom in Internet information appliances this year [see "Computing," pp. 45–50, and "Consumer electronics," pp. 51–56]

will soon have people worrying about addresses the way they did about Y2K: at the last minute. Fortunately, Windows 2000 should be released shortly and it supports IPv6.

Growing the address space is not the only fix needed. Today, the Internet works by having each router, or network node, try its best to deliver each packet of data, and treat all data packets as equal. So packets may be delivered higgledy-piggledy in no particular sequence or, even worse, not at all. While out-of-sequence arrival may not matter for electronic files that can be reassembled at leisure in a computer, it is disconcerting when it happens during an IP phone call.

For that reason, technologists working on the next generation of the Internet are experimenting with a new standard called differentiated services, or DiffServ. Created within the Internet Engineering Task Force, it will allow different kinds of traffic to be handled with different priorities, as well as allow businesses to offer users different types of service at different prices [see "Diversifying Internet delivery," *IEEE Spectrum*, November 1999, pp. 57–61].

If the tests begun in universities and research institutions last year succeed, this standard could start making its way into the public network this year. Such advanced

1. MODEM DOWNLOAD TIMES OF SHORT VIDEO	
Modem type	Download time for 7.5-MB video
6- [~] asynchronous digital subscriber loop (ADSL)	10 seconds
1- [~] /s ADSL	40 seconds
1.5-Mb/s cable	
128-kb/s integrated-services digital network (ISDN)	7 minutes
56.6-kb/s	18 minutes
28.8-kb/s	35 minutes

Source: ADSL Forum

work will not only supply universities with a solid research infrastructure, but also "stimulate creative students to invent applications that will sweep the Internet, as the World Wide Web did in the last decade," observed David Clark, senior research scientist at the Massachusetts Institute of Technology's Laboratory for Computer Science, in Cambridge, and a pioneering Internet developer. And attempts to increase Internet capacity, such as those mentioned by Vint Cerf of MCI Worldcom Inc., Clinton, Miss. [see "An interview with Vinton G. Cerf," pp. 43–44], will undoubtedly result in further evolution of the Internet.

CHANGE OF COMMAND

With luck, those technical changes to the Internet can be implemented in a stable political environment. Last year, the job of assigning Internet addresses was transferred from

The "Zaal" on the first floor is still preserved in the Louis XV style.

The "Zaal" on the first floor is still preserved in the Louis XV style.

The "Zaal" on the first floor is still preserved in the Louis XV style.

```

</div>
<div data-bbox="700 115 860 305" data-label="Text">


[1] The synchronized multimedia markup language, SMIL, makes it easier to create complex Web pages. In these screen shots—from a tour created by Oratrix Development BV, Amsterdam, the Netherlands—views of a Louis XV-era music room appear in the order a real visitor might see them. Image sequence and on-screen duration is specified in the source code [lower right]. The last image [not shown] is a video of a pianist playing the piano.


```

the Internet Assigned Number Authority (IANA) under the U.S. Department of Commerce to a newly formed not-for-profit organization: the Internet Corporation for assigned Names and Numbers (Icann). Despite the death of Jonathan B. Postel—who had been the director of IANA and ran it so effectively for almost 15 years—on 16 October 1998, the organization is managing to carry on with his important work.

As its name implies, Icann is also supposed to manage the registration of Internet domain names. In this process, a numerical address is connected to the www.anything.com names that the Internet has made a part of practically every advertisement. Previously, Network Solutions Inc., Herndon, Va., performed that function under contract to the U.S. government, and the company has not been eager to surrender the electronic tables that translate domain names to numerical IP addresses and that underpin its primary role in the working of the Internet.

It was not until September of last year—after a full year of legal maneuvering—that Network Solutions agreed to recognize its successor's legitimacy and turn the tables over to it. Even so, Network Solutions won the right to hold on to them for at least four more years to ensure a smooth transition. In the meantime, other commercial and non-commercial entities around the world will be able to register names in the coveted .com

domain. This year will reveal how smoothly that process goes and whether the Net can operate well with multiple registrars.

As a new organization in a new world, Icann is forced to invent itself as it goes and grows. The question of how its operations will be routinely funded—whether by government subsidy or a charge for the functions it performs—has yet to be determined, for now, the U.S. government is underwriting it. And that fact discomfits non-U.S. Internet interests, who want to have an equal say in the Net's running. Then too, ordinary Netizens would like to see the Net remain free from commercial control, yet it is unclear just how these average network users will be represented within Icann—as its charter says they must be.

In addition to dealing with these issues this year, Icann chair Esther Dyson will also have to wrestle with protecting intellectual property. People have been registering common brand names—like Coca-Cola, IBM, and McDonald's—as domain names without the trademark owner's permission [Fig. 2]. Although a recent U.S. case found that Network Solutions, Icann's predecessor, was not liable for registering a name that infringed on a Lockheed Martin trademark, inconsistencies in international laws are pressuring Icann to develop new policies for coping with such matters. It remains to be seen whether Icann or national legislatures will

have the final say in this matter.

One of the largest problems the Internet presents is how to apply laws to it, because it crosses all national boundaries. For instance, if one company wins a judgment against another in one jurisdiction, how can it collect if the loser is not subject to that jurisdiction? International laws and organizations have dealt with such trade problems in the past, but Net commerce will thrust them into the limelight, making flaws in the global legal apparatus blindingly apparent and invariably leading to international disputes.

The Net presents some truly new problems for business that must be dealt with by legislative bodies. For one, in the era of "digital ink" there is the issue of what constitutes a legally binding signature. In the U. S. Congress, the House and Senate recently passed separate bills that would make electronic signatures (information encrypted by a user with a private key that can only be opened with the user's public key) legally binding. European Union telecommunications ministers meeting in Brussels last month also approved a digital-signature law.

The U.S. government holds that it will do all in its power to encourage electronic commerce. Last September, it put its words into practice by loosening export controls on encryption hardware and software. At the time, Dave McCurdy, president of the Electronics Industry Alliance, Arlington,

VINTON G. CERF

continued

time and that means we have to start now. So another major challenge is figuring out a path to get from v4 to v6.

IPv6 is pretty dramatic and people haven't fully internalized how the routing and the allocations go and everything else. It's going to take time and I'm pushing hard to get busy with it.

How will the Internet affect the way we learn, work, and live in the next 25 years?

I've already seen the Net affect the way I work and behave. When I have a question, I find myself turning first to

the Net—I don't go to the library, to my bookshelf or to the telephone. Only if I can't find it on the Net do I start poking around in some of the older resources.

Even though you really have to think carefully about what you read, see, or hear on the Net, the richness of the space is just phenomenal. So while it's only a few years into this whole evolution, it's already having a major impact on the way I normally work and deal with information. It certainly has kept me in touch with friends and family.

I want to draw an analogy between the electric power distribution system and

networks that distribute information, in which computers—or “computing engines”—are the equivalent of fractional horsepower motors. I can foresee these knowledge motors being everywhere, doing knowledge work for us just as those electric motors do manual work for us.

What I hope is that this ability to place computing power in small quantities and communications wherever we need them will really result in some significant transformations. An application you're running might automatically negotiate for some outside services it needs and set them up on the fly, so you don't have to. Today, we're more involved in that than we need be. —R.C.

Va., and former chair of the House Permanent Select Committee on Intelligence, said, “[The] White House announcement recognizes that U.S. government policy desperately needed to catch up with reality.”

The reality was twofold. For one, non-U.S. companies were selling strong encryption products—ones using keys larger than 56 bits—both overseas and in the states, whereas U.S. firms could not sell overseas. So anyone who wanted to do business globally had to work with non-U.S. technology.

The second reality was that the U.S. patent on the RSA algorithm, a widely recognized strong-encryption public-key algorithm, was coming to an end, so companies all over the world would be free to implement it. Two weeks before the White House announcement, European researchers had shown it was possible to break that code when 155-digit numbers were used (albeit it took them five months using 300 PCs and a Cray 916 supercomputer). Thus companies will move to higher-order numbers, to 232 or even 309 digits, for encryption.

This year, the National Institute of Standards and Technology, Gaithersburg, Md., will be seeking comments on a new standard, the Advanced Encryption Standard (AES), which is intended to protect government information by using keys up to 256 bits long. From a field of 15, five candidate algorithms have already been selected. Three are from IBM, RSA Laboratories, and Counterpane Systems, and the others are from a pair of researchers in Belgium and a team from Israel, Norway, and the United Kingdom. The institute will accept comments from cryptographers reviewing the algorithms until this coming May, and make a decision by early next year. Like the Data Encryption Standard (DES) it will replace, the Advanced Encryption Standard will find use in the private sector; according to Secretary of Commerce William M. Daley, “The AES will serve as an important security tool in...electronic commerce.”

At the same time, the international com-

munity is finding better ways to ensure that systems are safe from malicious attack by viruses, Trojan horses, and the like. To this end, new standards for specifying and evaluating security needs, such as ISO IS 15408, are being ratified and adopted by corporations and governments worldwide.

Data security is not only important for commerce, individuals want to keep their information private, too. While encryption can ensure that information goes only to the intended recipient, also at issue is what the recipient is allowed to do with the information. For example, what use may a retailer make of information about what an individual looks at while visiting a Web site?

The issue of how to ensure individual privacy will come to the fore this year, as more people realize how nimble corporations can be at collecting private information on-line. In a recent incident, RealNetworks Inc., Seattle, Wash., was found to be surreptitiously gathering information on what users

listened to and saw with the company's RealPlayer software. RealNetworks rapidly issued a patch to undo the spying code so as not to lose its customers' good will and its market share to another supplier, such as Microsoft. Competition will demand smart use of precise demographic data, while not alienating customers through misuse of data about their on-line habits and preferences.

MONEY ON THE LINE

Another privacy issue is safeguarding financial and personal information that users might typically keep on their computers: home addresses and phone numbers, checking account numbers, passwords, credit card numbers, and such. Helping users manage this type of information is already a highly competitive business. Microsoft, Novell, and America Online are big companies offering such services, as are new Internet “pure-play” companies like Qpass, Clickmarks.com, and Zero-Knowledge Systems.

Personal information management is only one of the new businesses coming into existence because of the Net. Continuous on-line auctioning, as pioneered by eBay, is another. Brokering electronic design information and components, as QuestLink.com from QuestLink Technology does, is a third. Yet another is automated bargain shopping, created by priceline.com. The Net is an intrinsic part of these businesses; without it, the services could not be delivered at a reasonable cost. In truth, every type of business is being influenced by the Net.

Figures released last September at the European IT Forum in Paris by International Data Corp., Framingham, Mass., indicate e-commerce's compound annual growth rate is more than 190 percent. At the end of 1998, it was responsible for US \$50 billion and by 2003 it is projected to reach \$1.3 trillion. As fantastic as the latter sum may sound, Michael Capellas of Compaq Computer Corp., Houston, Texas, said at the conference that, in his estimate, IDC's projection seemed too low. ◆



[2] Is this trademark infringement? Ian Wong of Los Altos, Calif., says he registered the name “msdwnline.com” for his mountain-bike Web site. The Wall St. firm of Morgan Stanley Dean Witter & Co., New York, claims he's using its trademark.