



Fighting over the Future of the Internet

David Clark
MIT Computer Science
and Artificial Intelligence Laboratory

For much of the Internet's life, it has coevolved with the PC. The relative maturity of the PC could thus lead to the erroneous assumption that the Internet itself is mature. But as computing enters the post-PC era over the next decade, with mobile devices, sensors, actuators, and embedded processing everywhere, the Internet will undergo a period of rapid change to support these new classes of computing.

Even as the evolving nature of computing changes the Internet, the more important drivers of change are likely to be economic, social, and cultural. I have written previously about how a set of tussles among various stakeholders will define the Internet's future.¹ Going forward, what might those tussles be and what might they mean for the Internet?

As we predict the future, we should not underestimate the importance of cultural issues (and cultural differences in particular). Technical systems based on technical standards usually work the same everywhere. Such homogeneity can directly collide with divergent norms about such things as openness, privacy, identity, intellectual property protection, and, perhaps most fundamentally, the balance of rights between the state and the individual. One possible outcome is the acceptance of Inter-

net hegemony as a force for cultural uniformity. But, especially because that force is sometimes equated with the unwelcome cultural and political hegemony of the US – such things as our entertainment industry, our sports icons, and our fast food (not to mention our language and politics) – you can see the potential for a backlash that leads to a fragmentation of the Internet into regions, where behavior within regions is consistent with each region's norms, and connectivity is more constrained among regions. The drivers of this backlash would be nation-states trying to preserve their sovereignty and jurisdictional coherence, aligned with a grassroots desire to preserve cultural diversity. In a world where nations seem to fight wars as much over identity as economics, the alignment of these forces can have significant consequences.

Issues of economics and industry structure will also drive change. To model the future, it is helpful to catalog the tussles of today. There is a fundamental tussle between a core value of the current Internet – its open platform quality – and investors' desire to capitalize on their investments in expensive infrastructure. Examples include debates over network neutrality, debates over whether ISPs and their

business partners can profile their customers for advertising purposes, and the collision between the open Internet and more closed sorts of networks such as those for video delivery.

Looking forward, we must steer between two perils to reach a healthy and vibrant future. If ISPs, in pursuit of additional revenues, diverge from the Internet tradition of the open neutral platform and favor their preferred content and applications over those of unaffiliated third parties, it might reduce the rate of innovation, reduce the supply of content and applications, and stall the Internet's overall growth. On the other hand, if (perhaps due to regulation) ISPs provide only "simple dumb pipes," a commodity business fraught with low margins, they might not see a reason to upgrade their facilities, which could lead to stagnation in the capabilities or scale of the Internet. Both outcomes are unwelcome and feared by different stakeholders. In my view, there is a middle path that avoids both perils, but we will have to steer carefully down that path, especially if we are going to impose explicit regulation.

It is important to remember that the shape of tomorrow's ISP is not fixed and mature, any more than the Internet itself. Different business and policy decisions will have major influences on the future.

The packet layer of the Internet is not the only platform over which we will tussle. In the future, we might well debate whether higher-level application development platforms such as the iPhone or Facebook should be limited in the control they can impose. The Internet, taken broadly rather than just as a packet mover, is layers of platform on platform. One prediction about the future is that the debates will move "up" in the layers.

The research community today is exploring new concepts for networking, based on alternative modes of basic interaction – for example, delay-tolerant networks (DTNs), which relay data in a series of stages rather than directly from origin to destination, and information dissemination networks and "publish/subscribe" paradigms, which have a similar "staged" character. These modes will prove very important in the future Internet, and we will fight over whether they are competitive offerings "on top of" the basic packet forwarding paradigm or whether they become the basic service paradigm, in which case the owners of the network have the exclusive

ability to provide them. I personally believe that we will be much better off if application designers (and users) can select from a suite of competing service offerings at these levels. But this is just another example of the tussle over platform ownership.

To add another dimension to all these tussles, consider the future of the developing world. We have different governments with different cultures and rules of regulation, different users with different skills, using perhaps different platforms (such as mobile devices) with different histories of open access and business models for investment. The result is a rich and heterogeneous stew of expectations, onto which we will try to impose uniform Internet standards.

I mentioned that the future Internet will

**In the hands of government,
the Internet and, more generally,
the tools of cyberspace are a force
for centralized control.**

link not just PCs and PDAs but also sensors and actuators. An important tussle that we must anticipate is the one associated with the phrase "the surveillance society." Networked sensors have the ability to change society in fundamental ways, but those changes and the tensions they raise will have the power to change the Internet. At a technical level, the volume of data from sensors (including video monitors) could swamp the current sources of data today – business practice and human endeavor. At a policy level, one could imagine that the ISPs in one or another country are assigned to control access to various sorts of data (sensor and other), or alternatively, authoritatively add certain sorts of metadata to data from sensors. We must expect tensions over the embedding (or not) of data about geolocation, identity, information authenticity, access rights or limits, and so on into one or another protocol.

While I called the tussle over open platforms fundamental, the tussle between the state and the individual is even more fundamental. The Internet has been glorified as a tool for per-

sonal empowerment, the decentralization of everything, collective action, and the like. It has empowered nongovernmental organizations and transnational actors. But at the same time, IT is a tool for information gathering and processing, and modern government is essentially a data-driven bureaucracy. In the hands of government, the Internet and, more generally, the tools of cyberspace are a force for centralized control. So, we see the dual ideas of decentralization and user empowerment on the one hand doing battle with images of the surveillance society and total information awareness on the other. Are the individuals (and those who advocate for them) powerful enough to resist the tensions from the center? That is a critical question in scoping the future.

Finally (and perhaps beyond the time frame of these essays), we should ask what is next after the Internet has hooked up all the sensors, all the actuators, all the cars, and all the smart dust. The next step must be hooking up

humans. As we have more and more computers about us, and then inside us (as will certainly happen), all those computers will benefit from networking. This takes us to the debates over human augmentation, which will bring ethical and religious elements into the tussle. The future is going to be exciting. □

Reference

1. D.D. Clark et al., "Tussle in Cyberspace: Defining Tomorrow's Internet," *Trans. IEEE/ACM Networking*, vol. 13, no. 3, 2005, pp. 462–475.

David Clark is a senior research scientist at the MIT Computer Science and Artificial Intelligence Laboratory. His research interests include the future of the Internet, network security, and the implications of economics and society on technology. Clark has a PhD in computer science from MIT. Contact him at ddc@csail.mit.edu.

cn Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.

How far have we come?

See *IC's Millennium Predictions* (Jan/Feb 2000 special issue)

- "Guest Editors' Introduction: An Internet Millennium Mosaic": <http://doi.ieeecomputersociety.org/10.1109/MIC.2000.815848>
- "Millennial Forecasts": <http://doi.ieeecomputersociety.org/10.1109/4236.815849>

Where will we go?

See more from our *IC's Internet Predictions* issue (Jan/Feb 2010)

- "Guest Editors' Introduction: Internet Predictions": <http://doi.ieeecomputersociety.org/10.1109/MIC.2010.11>
- "Internet Predictions": <http://doi.ieeecomputersociety.org/10.1109/MIC.2010.12>

This article was featured in

computing **now**

ACCESS | DISCOVER | ENGAGE

For access to more content from the IEEE Computer Society,
see computingnow.computer.org.



IEEE  computer society

Top articles, podcasts, and more.



computingnow.computer.org