

Web 2.0 and Beyond: What Does the Cyber Future Hold?

Why This Matters

Web 2.0, the latest technology trend in computing and communications, is popular slang for a series of dynamic, interactive applications producing new forms of technological and social interaction. The lightning pace of Web 2.0 technological innovation and evolution challenges our ability—as individual users, communities (real and virtual), and cultures—to grapple with its immediate and enduring implications. As these technologies increase connectivity, decentralize power, and facilitate mass collaboration, cyberspace presents a formidable dilemma for policymakers: What does the future of cyberspace hold, and how might policymakers shape it?

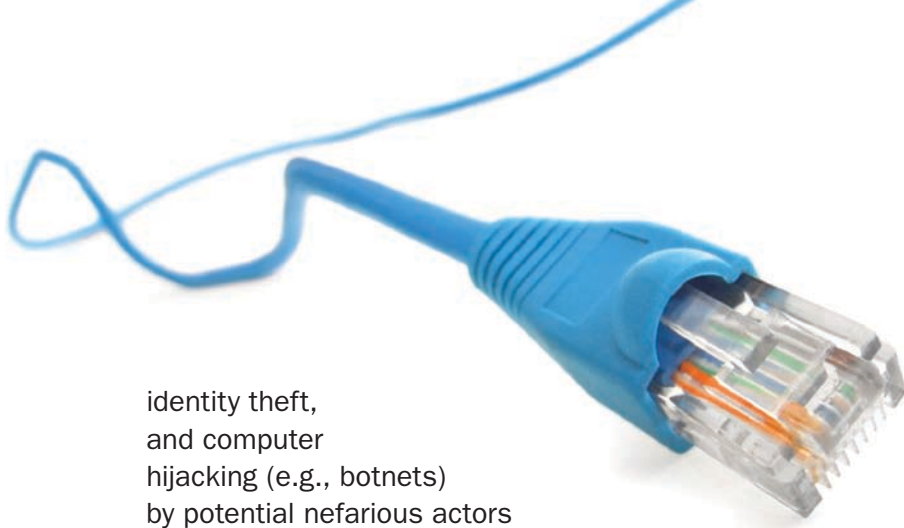
Control Protocol/Internet Protocol (TCP/IP), would have predicted the billions of global users taking advantage of the Internet today. They might not have fully imagined that Advanced Research Projects Agency Network (ARPANET), a network originally designed to connect researchers, would one day transform into a highly interactive, sophisticated communications medium that is a primary source for news, information, entertainment, and social interaction. They might also be surprised at how accessible the technology is, where highly educated professionals struggle with new software applications as their children and grandchildren immerse freely and easily into this new online world. Perhaps most germane, Cerf and Kahn might also freely admit that early on they favored a more open network architecture over a more secure network—a de-facto policy decision with cascading effects (both positive and negative) today.

What Is the Issue?

History has proven that predicting the future in cyberspace is folly. Each succeeding technology (and application and adoption) has spawned a spate of social-cultural phenomena, some of which have been natural, predictable progressions; others of which have been quite unexpected and even revolutionary. At the same time, however, far more than technology research and development cycles drive cyberspace. Market demands for speed, social desires for mobility, cultural aspirations for identity and connectedness, and political motives to raise money and reach new constituents pressure technologists to develop innovative hardware, software, applications, and content to feed our many appetites.

For example, it is hard to conceive that Vint Cerf and Bob Kahn, creators of Transmission

Today, leaders confront new choices about the future of the Internet, both in terms of difficult decisions made and deferred or avoided decisions. When a technology or trend takes hold in cyberspace, it tends to spread virally until it reaches a saturation point and then becomes part of the “cyberspace DNA” or disappears completely. The adoption of Web 2.0 functionality illustrates this point. Few question whether Web 2.0 adoption is an important development. However, some experts argue that Web 2.0 is fundamentally changing society’s relationship with the online world. These technologies and applications enable greater online collaboration and peer-to-peer networking and open new avenues for wealth generation. At the same time, critics point to new waves of exploitive social engineering techniques, data and



identity theft, and computer hijacking (e.g., botnets) by potential nefarious actors (e.g., individual hackers, criminals, terrorists, nation-states). To complicate matters, before we fully comprehend and develop policy frameworks to address these changes, speculation about the next wave, Web 3.0, already abounds—with its powerful semantic search abilities to link information, virtualization platforms promising even greater mobility, miniaturization and “nanoification” of computing technologies, 3-D interfaces, and explosions in devices “on the Net”—creating new challenges.

Consider the tradeoffs our leaders face today—preserving the open nature of the Internet, which fosters peer-to-peer collaboration; developing the Internet as a resilient, trusted conduit for global commerce; preventing the exploitation of vulnerable populations through social engineering, computer crime, and identity theft; protecting privacy and civil liberties; ensuring global Internet accessibility to enable the free flow of ideas and information across borders; securing the Internet in a manner that protects corporate America’s intellectual property and our nation’s critical infrastructure; retaining information dominance in cyberspace as a military force multiplier in the Global War on Terror; and hindering an adversary’s ability to exploit our cyber systems. Perhaps the most important tradeoff is determining the *appropriate roles of the public and private sectors in stimulating the future development of the Internet*. A reality and challenge in cyberspace is that leaders and policymakers come in many

forms—government officials, corporate officials who release new products, researchers who develop new code, individual users who express preferences online—and all make policy in an ad-hoc manner.

A series of cyber attacks in Estonia last year vividly illustrates policy challenges moving forward. Estonia is one of the world’s most connected societies (more than 90 percent penetration). Citizens young and old perform many of their daily functions (e.g., banking) exclusively online. The primary communications channel is SMS texting. Estonia is a culture deeply immersed in the Net Generation. During a period of heightened political tension between Estonia and Russia, a series of cyber attacks bombarded Estonian systems. Many critical infrastructures, including the financial services sector, were initially crippled. The computer attacks were believed to be Russian in origin, but attribution was impossible to determine (and 75 percent of those attacks came via U.S.-based IP addresses). The perpetrators employed a number of sophisticated social engineering tactics to further hamper recovery efforts (e.g., mass SMS texts to native Russians in Estonia encouraging them to take certain actions at designated times). The typical questions of “who is responsible?” and “who is in charge?” emerged as government, industry, and civil society struggled to deal with a cyberspace incident that quickly produced social, cultural, economic, political, and even military (the North Atlantic Treaty Organization was involved in the response efforts) responses with stunning speed and power.

The very nature of Web 2.0 forces one—policymaker, technologist, researcher, user—to think about the dynamism of the Internet. The policy dilemma appears to be

how to exploit the full range of the Internet's power yet reign it in when necessary to ensure it remains (in all of its complexity) a safe medium for commerce and social interaction. As a society, we are often so hypnotized by the sweeping popularity and advancements of new technologies that we fail to fully consider and address the accompanying risk. From a public policy perspective, we appear one or two steps behind, responding to effects instead of anticipating and influencing them from the outset. Given the difficulties of predicting cyber trends and the sheer speed of technological and socio-cultural changes in cyberspace, how can policymakers begin to shape the future?

Three Big Questions

- What do you see as the most important trend(s) occurring in cyberspace today? What are the implications of those trends? Are they largely positive or negative? Which present real opportunities for the future of cyberspace, and which present risks?
- What do you see as the role of government in shaping the Internet of the future? Can policymakers influence the future trajectory of the Internet? *Should they?*
- Is the notion of "Internet governance" an outmoded concept? What is the role of the United States in shaping the future of the Internet? How do others in the world perceive America's role vis-à-vis governing the Internet?

Panelists

- **Clay Shirky**, professor in the Interactive Telecommunications Program at the Tisch School of the Arts at New York University
- **Frances Townsend**, former assistant to President George W. Bush for homeland security and counterterrorism and former chairwoman of the Homeland Security Council

- **Paul Twomey**, president and CEO of the Internet Corporation for Assigned Names and Numbers (ICANN)

Moderator

Joan Dempsey, vice president at Booz Allen Hamilton

For Further Information on This Topic, Contact:

Joan Dempsey

Vice President
(703) 902-4100
dempsey_joan@bah.com

Dave Sulek

Principal
(703) 984-0798
sulek_dave@bah.com

