

### 3. Observations on Future Trends

**Observers: C. Richard Neu,  
Peter Denning, Raj Reddy, Lily Wu**

**Rapporteur: Richard Hundley**

The next session of the conference involved a panel of observers whose purpose was to expose and elucidate assumptions in the previous presentations of technological visions that may have gone unstated or unnoticed by the speakers; to call attention to clashes among the various visions presented; and to discuss whether these clashes may result from differing assumptions.

#### **Questions Posed by the Panel of Observers**

The panel of observers approached their task by posing a series of questions to the conference audience.

The first observer began by emphasizing the importance, in considering the various technological visions that have been presented, of distinguishing between:

- Human needs/wants that will almost certainly be satisfied.
- Things that may not happen.<sup>3</sup>

The question he implicitly posed was: Of the many technological visions presented thus far, which fit into each of these two categories?

The second point the first observer raised concerned the many “information utilities” contained in various of the technological visions. He posed the question: How will we protect these information utilities from “trashing”? (The analogy used was the degree to which public restrooms and public phone

-----  
<sup>3</sup> One example noted of “things that may not happen:” Widespread need for machine translation among human languages may be “trumped” by widespread use of English as a default language on the Internet and Web over the next two decades, if, as expected, these services spread primarily and initially to educated and elites of various countries that have adequate English comprehension.

booths in big cities tend to become defaced and “trashed” unless strongly protected by various access mechanisms.)

The second observer posed the question: Do we think it likely that Moore’s Law will continue for the next 15-20 years?

The third observer postulated a future in which there will be “infinite” memory and “infinite” bandwidth. As a consequence of this, he foresaw a future in which the broadcast industry will disappear and be replaced by “unicasting.” He posed the question: Is this plausible?

The last observer focused on *money* and *markets*. She put forward the following proposition: From all possible things that could happen, what is *likely* to happen will be determined by the availability of *money* and *markets*.<sup>4</sup> This led her to pose two questions:

- What are the funding implications/sources for all of the technology futures that have been discussed in the various vision statements?
- What will people pay for? What will be the profitability of various technology developments?

Putting a non-U.S. hat on, she also posed a third question:

- How will the technology trends that have been discussed play in the non-Western world, where there are different legal structures, different feelings about privacy, etc.?

## **The Discussion**

The remainder of the session was devoted to a discussion of these questions in which all of the conference attendees participated.

### ***The Future of Broadcasting***

One participant stated his firm belief that in a world of “infinite” bandwidth, broadcasting (i.e., the simultaneous transmission of the same material to many different individuals) will disappear and be replaced by “unicasting” (i.e., the transmission of material tailored specifically to each (and every) individual user). He cited “video on demand” as an early forerunner of unicasting.

---

<sup>4</sup> She gave as an example of this proposition in action the change in the business model in the semiconductor industry in the 1980s, when the development of “foundry” fabrication facilities changed the economics of semiconductor design, development, and production.

Another participant reminded the audience of the impact of the printing press on society -- the last great information revolution in his view -- where contradictory effects happened simultaneously. The implied lesson he draws from this: We should be cautious in making dogmatic predictions about the future of "broadcasting," "unicasting," etc.

### ***The Future of Moore's Law***

One of the conference participants gave the following as the reason Moore's Law continues to work: The process (of semiconductor development) involves a number of separate, complex steps with a number of layers that can be independently improved. He cited biotechnology as another technology that could be subject to a Moore's-like law in the future.

Another participant noted that if Moore's Law were to continue unabated, in 2017 the individual feature size would be at the one-electron scale. The conclusion he draws from this: To continue Moore's Law unabated, we will have to leave silicon.

Still another participant noted that the big change (i.e., from individual transistors to integrated circuits) leading to Moore's Law came from the miniaturization of chips. In his view, sooner or later this will reach physical limits. When this happens, Moore's Law as we know it today will reach a limit, insofar as hardware is concerned.

### ***Security of Information Utilities***

One of the conference participants asserted that we have the technological capability to have adequate security for the information utilities and for other aspects of the information world. In response to this assertion, another participant noted that most of the computer security technology available today is not used on most of the computers in the world. He posed the question: Will this change over the next 20 years, and if so, why? His implication: if usage doesn't change, we may never have adequate security.

A third participant answered this question: Yes, this will change -- because we are now assigning economic value to transactions in cyberspace.

Elaborating on this, another participant noted that the scientific community, which initially developed the Internet, focused on authenticity and speed; e-commerce has a different security focus.

Elaborating further, still another participant mentioned that up to now IT developments have been driven by a community (i.e., academia) that was not interested in practical security. Sooner or later, in this person's view, IT development leadership will be taken over by the non-academic (i.e., commercial) community, which is interested in practical security matters.

Still another participant argued that this speaks to the security (awareness/performance) of individual organizations connected to the Internet. It doesn't speak to the collective security aspects of the net.<sup>5</sup> To achieve an adequate level of collective security, she believes we need regulations for the security levels of entities connecting to the Internet.

Another participant explained that besides *security*, we need *trust* and *confidence*. According to this participant, E-bay and others are developing (or have developed) procedures to provide trust and confidence in Internet transactions.

Responding to this, the previous participant noted that *reliability* is also a problem. Today, reliability levels of computer systems fall into two distinct classes:

- Personal computers and small business computers, for which the achieved reliability levels are often low.
- Computer systems owned and operated by large organizations, for which the achieved reliability levels are usually high.

These differences occur because large organizations usually treat reliability and security in a more thoughtful, careful, complete manner than do small businesses and individuals.

Elaborating on this thought, another participant mentioned that the large multinational business organization of which he had once been a part treated risk management (of computer-related risks and other risks) in a very formal way. It drew profiles of the various things that could go wrong, assigned economic value to each of these risks, and assessed its capabilities to mitigate each risk. It did this once a quarter.

Still another participant said that the free market has mechanisms through which companies can offer effective security services, privacy, etc., *provided that governments and/or monopolies do not limit the technologies available.*

---

<sup>5</sup> By the collective security aspects of the Internet she means situations in which a malevolent actor uses a security hole in party A's systems to cause damage not to party A but to party B, who could be on the opposite side of the world, totally unrelated to party A.

It was suggested that in the future, we should expect many more unconfigurable information devices or appliances, so that their security and reliability can't be compromised. (It is not clear, however, whether unconfigurability precludes various types of denial of service attacks.)

Another participant pointed out that there appears to be a market failure today. For security to sell, it has to be bundled and unobtrusive. Otherwise, people usually won't buy it. Another aspect of the market failure is that we can't today adequately measure risk, and therefore don't know how to value security.

Still another participant mentioned that market failures similar to this (i.e., safety or security problems) have occurred in the past in other industries. Effective solutions to such previous market-failure problems have usually involved:

- Public pressure by advocacy groups.
- Some form of government regulation, in response to this pressure.

He cited the impact that Ralph Nader (e.g., *Unsafe At Any Speed*) had on auto safety in the U.S. as an example of this phenomenon.

As a final word on the subject of security, one of the conference participants stated that: "Information security has got to get better. Therefore it will get better." (In other words, if it's required, it will happen.)

### ***Other Drivers of Change***

Changing the subject (somewhat), another conference participant noted that the entertainment industry -- which had not been mentioned up to now anywhere in the conference discussions -- will be an enormous driver of future technological change in the information world. This thought led the participant to pose a broader question: What are the different communities (in the information world) that will grow in importance over the next 20 years? He noted that these various communities may/will have different values, and these different values will shape the course of future change.