

4. Technology Trends and Artifacts

Group Leader: William Caelli

Rapporteur: Jonathan Caulkins

The charter for this first breakout discussion group was to consider in more depth the various technology developments likely to occur in the next 15-20 years, then to consider specific artifacts likely to emerge in that time period as the result of those technology developments. Emphasis was to be placed on artifacts that have the greatest potential for affecting the lives, relationships, and business dealings of individuals, organizations, and countries or regions – with special attention to those that might have differential impacts across regions, cultures, or other boundaries.

The group, in a fairly open-ended brainstorming fashion, identified ten key technologies/artifacts that “will happen,” isolated a key assumption underlying those predictions, and listed two “tensions” whose resolution would affect what transpires in 15-20 years. Based on these observations, the group then sought to synthesize visions of the new worlds of physical systems, computer code, and human interactions.

Technologies/Artifacts that “will happen”

Over the next 15-20 years, literally thousands of new information technology-related artifacts will be developed, marketed, sold, and distributed widely. This breakout session could clearly not predict or list anything more than a very small selection. The following artifacts were chosen for discussion, as exemplars of likely futures that seemed particularly important – at least in developed countries – and not universally appreciated.

Developments

1. *Digital personas.* These are personalized databases or “agent” programs that accumulate a history of the location, movement, actions, and

environment of an individual. Much of this data is being collected now, e.g., in computer browser “cookie” files, in geographic tracking information generated by cellphones, and so on. The limits to the spread of this type of artifact are legal and social. The advantages of the personalization and tailoring of transactions made possible by such “digital personas” will encourage their spread, subject to some modest limitations. (But note an earlier comment in these proceedings that one person may develop – perhaps even cultivate – several such digital personas, providing some degree of privacy for some realms of activity.)

2. *High-resolution portable displays and wearable computers.* With continuing advances in wireless communication (see section 2 on Communications Technology), individuals will increasingly want continuing access to information resources while mobile. “Wearable computers” of various types – including “smart clothing” with embedded sensors connected to computing and communication resources – will proliferate.
3. *Major advances in input modalities.* This is an extension of the wearable computer concept to input/output devices (some portable) that enhance the user/computer interface by including all the senses: visual, audio, tactile, smell and taste. The group discussion even touched on monitoring of brain wave activity and rudimentary thought transfer, but there was much scepticism about how far these developments would extend by 2020.
4. *Ubiquitous, smart sensors and wireless connectivity.* This is perhaps the area with the greatest possible impact in about 20 years. If, as expected, some useful sensors become mass-produced to the extent that their per-unit cost is one dollar or less, they will become ubiquitous on devices, artifacts, clothing, and perhaps as embedded sensor/monitors. Their viability would be improved if the sensors could extract power for their operation from their environment. The largest impact may be in medical applications, but the conservative regulatory environment concerning medical innovation suggests that initially applications may focus more on: smart materials, construction uses, wide area networks for environmental sensing, and so on. To some extent, current international frequency spectrum allocation approaches will limit wireless capabilities, but as mentioned in Section 2 very localized wireless protocols such as Bluetooth can enable such sensors to communicate to a local “hub” (e.g., within 10 meters) that in turn is connected to larger networks. One uncertainty involves the long term medical consequences of these radiofrequency emissions on humans. We need better understanding of the biological effects before use of wireless

systems – especially those in close contact with humans – becomes ubiquitous not only because of the “objective” risks but also because of the possibility that “irrational” or media-hyped fears of such risks would block widescale deployment even if the risks are not in fact large.

5. *Soft control of hardware.* The U.S. military is investing heavily in software-controlled radios. This is one small example of hardware that is substantially reconfigurable through software, allowing devices to evolve more gracefully to keep up with the rapidly changing demands of the information revolution. Such greater software control of hardware will increase.
6. *Ubiquitous digital access to the net.* As mentioned elsewhere in this report, widespread accessibility of “the net” from a rich variety of devices and locations is a common prediction. One highly-prized application would be the ability to anonymously browse the net. This is technically feasible, but subject to possible legal and social constraints yet to be worked out. The outcomes may well differ among countries, regions, and cultures.
7. *Collapse of the switched network.* If traditional switched telecommunications service (such as traditional voice telephone service to homes) is replaced in most locales by packet-switched technology, there are implications for the urban vs. rural digital divide. When most people bypass switched services, how can costs be recovered to support the remaining pockets of subscribers not yet reached by broadband packet services?
8. *Trusted mobile code.* Mobile code is software that migrates over networks to various client machines, for local execution. An example is an e-mail attachment that executes in some manner when accessed – for example a Word document with embedded macros that launch when the document is opened. Such mobile code is currently a major source of virus and worm attacks. The discussion group expects protocols and safeguards to be worked out so that mobile code received and executed under normal conditions can be trusted. The problem is more administrative and procedural than technical.
9. *Major advances in computer mediated human interactions, particularly asynchronous ones.* Electronic mail (e-mail) is a common form of asynchronous computer-mediated communication. It is the most widely used application on the Internet. The group felt that major advancements in such asynchronous communication were likely. (Video conferencing will become commonplace also, but it is deemed a less important revolution than

advances in asynchronous interaction, due to the major advantages of asynchronicity in human communication.)

10. *Great imaging interfaces.* Visual displays provide tremendous bandwidth between computing and communication devices and their human users. Because of the importance of these displays to the whole user-computer interface experience, they will continue to improve in resolution, size, thinness, and other useful attributes. These developments will be spurred by the entertainment industry and its high-definition TV, gaming systems, and the like.

Assumption

A major assumption underlying the above developments that was highlighted by the discussion group is that: The US government will succeed in establishing necessary commonalities to avoid balkanization from desires for proprietary control leading to multiple protocols overlaid on top of each other, which would be a major problem. The word “commonalities” was selected over “standards” intentionally. The feeling was that ANSI, ISO, etc. would not be the key, but rather that implicit or explicit government sanction of particular approaches would, via first mover advantage, focus the market’s efforts on one architecture, language, protocol, etc. over another. It was observed that it is getting harder to tip the market by being an early trendsetter because the big firms in the private sector move so fast, and government has withdrawn from the roles of ensuring safety and security that it plays in other sectors. A subset of the group argued that the US government has historically played this role (e.g., through DARPA) and would continue to successfully walk the line between meddlesome interference (as sometimes exhibited, for example, by Singapore) and a completely laissez-faire approach (e.g., the approach often taken by Australia). Another faction pointed to the inability to write Postscript files from new versions of Word as a worrying portent of a less optimistic future. The group concluded that:

“In its role of helping to improve the innovation process, the government will help guide the development of interfaces that enable multiple interactions of artifacts. Rapid change in the marketplace leads to unpredictability, which deters development of useful interface guidelines.”

The question and answer session when these results were briefed to the larger conference indicated that others were skeptical of this rosy view, preferring perhaps a statement that the government “needs to help guide the

development” of these interfaces, not that it necessarily will do so wisely. It is a key assumption, not an innocuous one.

Tensions

Two tensions resulting from the above developments were highlighted by the discussion group: ones involving open vs. closed “worlds,” the other involving the strength of intellectual property right protections.

1) *Open vs. Closed worlds.* Powerful trends/incentives were seen pulling toward both the closed and the open end of the spectrum, dubbed the “Windows” and “Linux” scenarios. The image of the closed world was “shrink wrapped” products that would not allow users to “look under the hood” or tinker (tamper) with underlying “code.” The prototypical example is Microsoft’s unwillingness to sell its assembler. The open image was a “new regime of simplicity” in which the drivers are trust, mobility of code, and linking of applications. A statement by one participant was that “The days of the non-sandboxed interactions are numbered and PEPC (privacy enhanced personal computers) will be the norm.”

There was no consensus on which trend would “win.” Indeed, there was a reluctance to see this as an either/or proposition. The “market share” of the two approaches might cycle, or perhaps it would always be possible to “own the code” but only by paying a “hit on capability.”

2) *Strength of IP (intellectual property right) protections.* The group believed that IP rules in a web-world are still up for grabs in important ways, and the future depends very much on how the law comes down. Two examples of the uncertainty were: (1) Caching and fair use. Libraries do not violate copyright when they loan a book because that is “fair use”. When persons download information from the web, they are making copies (on their machines, on mirror sites). Will that remain within fair use? (2) Is it legal to make a pointer to Napster? There was a notion that at present it is OK to make a pointer to its head but not using “deep linking” -- but one could imagine more such “test cases” in the future.

The group saw a trend toward more power for IP holders. “We’re creating legal and technical mechanisms that enhance the ability of IP entities to retain control. That runs counter to the openness of the internet.”

Developments most likely to occur, and most consequential

When asked to select and detail the technologies/artifacts that are “most likely to occur” and whose occurrence would be “most consequential” the group selected three visions of a “new world.” The consensus of observers is that the group, perhaps unconsciously, defined these criteria as “most likely to be technically possible within the forecast horizon (e.g., 15-20 years) and to be most consequential in the long run,” not as “most likely to have become most consequential within that 15-20 year time horizon.”

They chose to present their deliberations in terms of three “new worlds:” the New World of Physical Systems, the New World of Code, and the New World of Human Interaction.

The New World of Physical Systems

The group believed (as outlined in Section 2) that we are on the verge of a revolutionary explosion in sensor and wireless communication capabilities and reduction in cost to achieve those capabilities. This “New World of Physical Systems” vision emerged by building on that premise. It is defined as “The existence and deployment of active/passive sensors, communicators, and related devices with associated (wireless) communications capabilities that make participation in an information environment fully possible – with embedded knowledge and information models to know how to use all this information.” Smart highways and smart houses/offices are signal examples. (Note: the notion of smart structures wasn’t confined to such visions as refrigerators that automatically order groceries. It includes smart materials and structures that adapt to physical stresses, e.g., materials that sense they are near the onset of failure and smartly repair themselves such as might occur in earthquakes or, chameleon-like battle tanks that blend in with their environment.)

The breakthrough technology was the capacity to saturate physical space with sensors that have embedded “knowledge” of the information environment in which they are deployed. (There was no consensus on whether this intelligence would be centralized or distributed.) One of the key limiting factors of this new world of physical systems is the inability of the international community to come to grips with the issue of spectrum usage among countries, so wireless systems can operate anywhere in the world without interference effects. It is a politically driven issue, since the

international governing body charged with this problem cannot agree on procedures for sharing the spectrum across national boundaries.

The overall group feeling about this New World of Physical Systems was: “This changes everything.” However, the group spent little time elaborating on this statement precisely because the effects were so numerous.

The main effect of this vision is a strong coupling of physical and cyber space.

A key tension was that too much information can lead to privacy concerns (think “The Truman Show”) and legal liabilities. (If the sensor owned by an entity knew of some threat, flaw, or presence, then it might create legal liability for the owner if that threat, flaw, or presence led to harm.) The optimistic view was that any individual could at any time say “sensors off” to protect privacy, but that could render ubiquitous sensors moot in public spaces where there might almost always be at least one privacy advocate. The ability of the legal, social, and political systems to cope with this new world was doubted, but there seemed to be an implicit assumption that the technology would win.⁶

The group briefly discussed possible differential regional effects of this New World of Physical Systems. They felt that participation in this sensor-laden environment could become compulsory in regimes without privacy protections (China?) with 1984-like implications. Group members said, “Imagine the threat from micro-cameras and then multiply ten-fold.”

There was discussion of how long it would take for a “Moore’s Law of Sensors” to make sensors so common (to the point of disposability) that this vision would be realized. The notion was that when cost is reduced to \$1 - \$2 we’d have reached that stage. That is, the key metric does not pertain to the accuracy or precision of the sensor, but rather to yield of usable units per wafer. That will be achieved sooner for some types of sensors (accelerometers) than others (medical sensors). Specifically, the expectations for such inexpensive, mass-produced and ubiquitous sensors were:

- Accelerometers (now)
- Food spoilage detectors in plastic food wrap (now)
- Gyroscopes (1 year)

⁶ Aside: The rapporteur’s personal view is the opposite, that legal and privacy constraints (as well as the constraints of legacy physical infrastructure) will mean only private spaces inhabited by first-world people from the upper half of the income distribution will be saturated with these networked sensors within the next 20 years. Non-networked (less intelligent) sensors (along the lines of lights triggered by motion sensors and automatic traffic signals) will be the more common form in public spaces.

- Cameras (3 years)
- MEMS microphones (3-4 years)
- Smell (e.g., for bomb detection) (5 years) – Smell actuation will be longer than detection
- Bio-sensors (e.g., for Legionnaire's disease) 5 – 20 years
- Medical (10 – 20 years)

In addition, polymer-based sensors were also noted by an expert as being a very important development.

It was felt that the bio/medical sensors will take longer to develop because of FDA regulations and concerns. Also, part of the vision involved sensors being fairly autonomous with respect to their power source. There were conflicting statements about whether that might be a constraint. The group was not very clear as to whether the times estimates shown above are unconditional, or whether they are conditional on advances in power sources for applications in which the sensor would not be connected to some external source of power (whether electrical or mechanical, such as deriving power from being part of a moving object). One of the tradeoffs is how much information processing and storage is put into the sensor device itself; more intelligence in the sensor will inevitably lead to lower communications requirements, which can in turn reduce power requirements. The group didn't have time to explore this issue in depth, but it is an important tradeoff that must be considered.

It was noted that the automobile industry could be key in pushing low-cost sensor technology forward because they use sensors in large enough numbers to push costs down the economies of scale curve. (This is already the case with sensors in air bags and accelerometers in automated braking systems (ABS); the next generation of cars could have gyros in ABS as well.)

The New World of Code

There is a trend toward more explicit management and representation of trust and verification, analysis, and encapsulation of mobile received code. These characteristics are currently used to assure that the code does not do something it shouldn't, but will eventually also apply to making sure it does what it's supposed to do. Developments in this area will allow construction of large-scale, distributed, component-based, multi-sourced, trustworthy code. This accomplishment rests on five related developments:

- Development of trust-supporting networks, which include the local (client) operating system. This is a matter of changing conventions and implementing technologies we have now. It involves configuring existing

systems for privacy and security, and the emergence of safety-enhanced Internet Service Providers (ISPs).

- Client-side means of proof and verification, including better understanding of methods and procedures for evaluating received code – such as better “sandboxes” that provide absolute safety for small pieces of code.
- Means of becoming certified as a trustworthy provider of code (e.g., by certifying the provider through a third party like Underwriters Laboratories).
- Compilers and structures that allow software producers to produce trusted mobile code. That is, an enabling technology that lets people produce and verify the software components themselves.
- Articulation of security and privacy policies and reasoning about those policies, advanced sufficiently to support the other aspects of this prediction. (There was a notion that “Implementing security and privacy is easy; defining, articulating, and reasoning about security policy is hard.”) There was also discussion that two possible ways of achieving safe use of received code are: (1) prevention techniques, and (2) mitigation techniques. The latter recognize that damage done by failures is usually bounded, and so it should be possible to develop procedures to repair these failures. This leads to the strategy: prevent, detect, tolerate.

If this New World of Code becomes viable, it was felt that tradable/trusted code will be a major enabler, along with robustness, for all industries and sectors that use information technology.

What might be regional/cultural effects of these developments? To the extent that we develop client-side means of proof and verification (e.g., through “sandboxes” or similar methods), it might help small countries or new suppliers to sell IT products, because without these breakthroughs there may be a tendency only to buy from name brand producers.

An assumption underlying these developments is the need for the next generation of compiler and software generation tools, and reversal of the trend of lack of attention to configuration management.

The New World of Human Interaction

New systems will be developed to revolutionize human-to-human contact and interaction, particularly in asynchronous communications with appropriate

parameters of discourse. Enabling collaboration often focuses on video-conferencing (a synchronous technology), and the group believed that better video 20 years from now is a given. But there was a notion that the bigger payoff will actually come from improved technologies for asynchronous interaction, since most work interactions are in asynchronous mode. The motivating example is an observation made by one of the group members that email hasn't changed a bit since he started using it in 1973. The average e-mail user has 200-300 threads going at once, and the best technical support is "raw" searching. There are great inefficiencies in a user's constantly context switching among various threads of discourse in which he or she is involved.

Other examples offered were the need for better calendaring, intelligent chat rooms, and "family reunion sites".⁷ The idea is that the latter could find commercial applications in domains such as reducing medical errors. More widespread application of methods such as used by moviecritic.com was also mentioned.⁸

Discussants thought widespread use of these developments could have an "incredible" effect on the work environment.

There could well be differential regional effects in use of these developments, because there are regional differences in work habits and mores. Although the group mentioned various possible regional effects, there wasn't the time or empirical basis for evaluating the different stories. A possible effect might result from efforts to bridge between cultures by enabling communication among workers who span cultures. These cultural differences might make it harder to develop the tools for small-market cultures (a possible advantage for the US) or they might help break down barriers between cultures. Analogies were made to machine translation of culture as well as language (to the advantage of small-market cultures). On the other hand, these tools might promote a single, global work culture in the way that English is emerging as the *lingua franca* of commerce and science. If that were to occur, US mores might be disproportionately represented.

The main assumption underlying the above "world" is that our understanding of human interaction and work processes will advance sufficiently. That is, the

⁷ These were discussed as sites where members of a group (e.g., an extended family) can post and share information among themselves, the way people do for funerals, weddings, and the like.

⁸ The "technology" involved is using your stated preferences with respect to some domain elements (e.g., movies) to match you with other respondents for purposes of using their opinions of a domain element you haven't sampled to predict how you'll react to that domain sample. I.e., instead of assuming Roger Ebert knows your tastes, you search over a large population of respondents to find kindred spirits.

technical hurdle is probably not in the software engineering but in the sociology. However, the market demand is huge: So many people use email that a major improvement in one's efficiency at processing email would have a lot of buyers. So nontrivial investment in this development could be justified.