This article is part of the IEEE Reliability Society 2009 Annual Technology Report.

# Technology Trends in Mobile Communication: How Mobile are Your Data?

Christian K. Hansen
Eastern Washington University
Email: c.k.hansen@ieee.org

**Introduction**

Over the last two decades, communication has become faster and less expensive, and communication systems continue to become increasingly portable, networked, and integrated. Ultraportable Mobile Internet Devices (MID) [5], [6] have allowed professionals to easily bring their work with them on their daily commute, and/or when traveling. These devices offer users the capability of using the internet, connecting with the office e-mail, network calendar, and time management systems, as well as providing a variety of entertainment functions, including audio, movies, and gaming applications while on the road. We have seen communication and management systems develop in at least four different directions:

1) from paper-based to electronic systems (calendars, time managers),
2) from desktop to (ultra) portable systems,
3) from personal to shared (networked) systems, and
4) from independent to integrated systems.

While it appears that in many ways our access to technological gadgets now exceeds our imagination, the developments of communication systems in these four directions give rise to two important questions:

1) While the communications hardware has clearly become reasonably portable, how portable are the software applications and data?
2) Increased portability has created increased vulnerability; but has the technology fully addressed security and reliability issues created as result of users carrying all of their company's sensitive data in their pocket or purse?

As I address these two questions in this article, I will look closer at the trends in each of these directions, and offer some predictions and "wish lists" on development still needed for the communications technology to reach full maturity.

**From paper-based to electronic systems.**

In the 1980s, the leather-bound paper-based planners with calendars, to-lists, planning notes, etc. gained wide popularity among managers and executives. Like many other people, I recently transitioned from using my paper planner in favor of an all-electronic system, but there are still features of the old paper planner that I miss. Apart from the ease of navigating through a paper calendar, or the ability to collect family photos and business cards in its pockets, the reliability of the paper planners appear to be far superior to the new generation of electronic planners. Paper-based planners do not run out of battery power, or crash during important meetings; neither do they contain parts that exhibit significant wear over time. Overall, the decision to move from paper to electronic planners has offered little or no advantage aside from those given in the three trends noted below.

**From desktop to portable systems.**

Surveys reported in earlier time management literature frequently cited "travel" as one if the top 20 biggest time wasters. According to more recent surveys published in the 4th edition of "The Time Trap" [4] this thought is no longer held in common, and mostly this change is due to the access to increasingly portable and wireless electronic devices, allowing anybody to bring work with them, and stay in touch by phone or e-mail anywhere, anytime. While this trend may continue, there are still some advantages that desktop systems offer over ultraportable (fit-in-your-pocket) systems. Full size keyboards and multiple

monitors provide a much more effective work environment than does the typical 15" screen of a laptop computer, or a 3" screen of a PDA.

**From personal to shared systems.**
How much time do we currently waste setting up meetings because not everyone is part of the same calendar network? Today's technology offers us the capability to instantly schedule a meeting time and space with a few clicks of a mouse. This is clearly a feature that offers a strong reason to abandon the old paper calendar. While the technology for doing this has reached maturity, it has not yet been widely adopted. The issue seems to be more culture than technology related. Many people are reluctant to adopt electronically shared calendars due to issues of privacy. They don't want other people to know if they are in the office, on the golf course, or on vacation. Yet the technology has already addressed many of these concerns, allowing users to set appointments to "private" or "hidden". In fact, shared calendars offer a much higher level of privacy than a paper calendar. Business and academic leaders and managers have a higher responsibility for the development of the new networked calendar culture than the developers of the technology. More effective scheduling systems could potentially save thousands of hours for organizations, although professional secretaries and administrative assistants may see this as a threat to their profession.

**From independent to integrated systems.**
Developments in this direction appear to be happening slower than in the other three directions mentioned above. Approaching the year 2010, there is still a distinction between a TV and a computer, and between a cell phone and a landline telephone, even though these devices share the same networks. On the software side, we are experiencing a much faster convergence towards systems integration. We have seen an integration of e-mail, voice & text messages, calendars, project and time management systems take place over the last few years with Microsoft Outlook [1] occupying the largest market share. Further integration with financial management systems (payroll, billing), web content management systems, and in higher education, student information and course content management systems will be highly demanded over the next decade.

**How Portable Are Your Data?**
Most professionals work on their data files through multiple workstations. The ultraportable PC or smart phone is useful for sending basic e-mail messages, setting up appointments, and reviewing a to-do list while working in tight spaces like in the doctor's waiting room, while commuting, etc., but it is not ideal for working in the regular office. Most people prefer an office computer setup that includes a full-size keyboard, and multiple large-size monitors, as well as a variety of peripherals including scanners, printers, etc. A regular size laptop with a 15" monitor may be an appropriate compromise between portability and usability for many people, but most people would prefer to be able to transition seamlessly from one workstation to another without having to worry about the transfer of data between workstations. Unfortunately, the technology that allows users to seamlessly carry data with them has not yet reached maturity. There are four methods commonly used for this purpose, but each method offers both advantages and disadvantages.

<u>Method 1: Carrying data on a USB drive</u>
USB drives have inherited the roles of the floppy disk (1980s), and the compact disk (1990s); and like these media of the previous generations, they offer an inexpensive method for taking all important data on the road. Most users can fit all of their necessary data on a 16 or 32 GB drive, which conveniently fits on a keychain. USB is an industry standard, so it requires no special network access or special software. The biggest disadvantage of a USB drive may be its high vulnerability. A lost or stolen USB drive could be disastrous, and a damaged device that is not backed up could result in loss of all data. Those who use USB drives to store their data must take two precautions that both limit the convenience of this method. One precaution is to make frequent backups of the data on a host computer, or a portable hard disk to prevent loss of data in case of a lost, stolen, or damaged USB drive. There are various utilities available

(some of which are free) that allow for synchronization between multiple media (see method 3). Another precaution is to use (hardware or software) encryption to protect sensitive data in the event of a lost or stolen USB drive. TrueCrypt (www.truecrypt.com), and other companies offer free encryption software utilities. A less significant disadvantage is the lack of portability of software applications. There are some utilities available that allow applications (even entire operating systems) to run off the USB drive, but as of today, many applications are not supported.

Method 2: Using a Remote Desktop

With this method, all data and applications reside on a host computer, e.g. the workstation located in the user's regular office. Through the remote desktop software, the user logs on to the host computer usually through a virtual private network. Some software allows secure connection through a web browser. The advantage of this method is that all data and applications are protected as long as the host computer remains in a "safe location." There is little or no potential for loss of data in the event of a lost or stolen portable device, except when the device is stolen while actively connected to the host. Because applications run off the host computer, there is no need to maintain identical software on each computer that is used to access the host. A disadvantage of this method is that the user has to be on a network to access the host. Until the entire world has become wireless, this poses serious limitations for the user. There has been talk about providing wireless connectivity on airplanes, but it will probably be awhile until wireless access becomes widely effective. Another limitation of the method is that many companies and organizations impose restrictions on the capability to remotely access their computers.

Method 3: Synchronization of Two or More Computers

With this method, identical copies of the same data reside on two or more workstations. Synchronization can be performed through a network using software such as GoodSync Pro (www.goodsync.com). Unlike the remote desktop method, a workstation can be used without a network (after synchronization), and the portability of data is much more seamless than with the USB drive method. Another advantage of this method is that backup is made continuously. If one computer is lost, stolen, or damaged, most of the data can be recovered from another computer.

Like with method 1, a disadvantage is that the applications are not (as easily) synchronized. Also like method 1, sensitive data need to be encrypted unless the device is anti-theft protected. Like method 2, some companies may impose restrictions on the ability to synchronize sensitive files such as files used by Microsoft Outlook.

Method 4: Using a docking station

Some manufacturers offer an optional docking station or port replicator that allows the user to connect external devices (keyboard, mouse, monitor(s), powers supply, etc.) to the laptop through a single connection. A limitation of this method is that port replicators (with a single connection) are not available for all makes and models of laptops, e,g. due to a lack of standard for external power supplies. Also, for the highly mobile professional who needs to dock/undock his/her computer 10-20 times per day, the heavy usage of the connector that connects the computer with the external devices can be quite significant, leading to high probability of failure within a typical laptop's useful life.

**Anti-theft Protection**

Every 53 seconds, a laptop computer is stolen from an airport terminal, or other public locations [3], [7] . With the new Intel anti-theft technology [2], a laptop computer or mobile device that is reported stolen can be rendered unusable through the sending of a "poison pill." While in this disabled mode, the computer will not be able to boot even with a replaced hard disk, and GPS technology will further allow the stolen device to be tracked to its location. Once a laptop is recovered, the data can then be unlocked. Although this offers some protection against theft, it does not safe-guard the data on the computer from being lost unless backed up on another computer. In fact, it is quite likely that the stolen device after being rendered unusable is directed to a garbage can or a landfill rather than being returned to its owner.

A desirable feature would be to also have the data of the stolen laptop transmitted to a "safe location." This feature appears to be easily developed using the same technology that triggers the "poison pill."
Users of laptops not equipped with anti-theft technology may want to secure their data through the use of encryption as previously mentioned. Yubikey [8] is a convenient device that can be used to quickly decrypt a computer simply by plugging the device into the USB port. Obviously, unlike the "poison pill," this method does not protect a laptop that is stolen while it is in use (e.g. from an airport).

**Conclusions**

Technological improvements observed over the past two decades have offered substantial advantages in our ability to communicate effectively, and in our access to information. In the next decade of technology development, I predict that major advances will be needed in each of three areas:

- increased security and privacy protection of data,
- increased wireless connectivity, and
- increased portability of data in using multiple workstations by the same user.

**References**

[1] Boyce, J. (2007) Microsoft Office Outlook 2007 Inside Out, Microsoft Press
[2] Hachman, M. (2008) Intel Details Plans for Laptop Anti-Theft Technology, PC Magazine Digital Edition , April 2008
[3] Hachman, M. (2009) Lost Notebooks Cost Corporations $50K Apiece, PC Magazine Digital Edition , April 2009
[4] MacKenzie, A. and Nickerson P. (2009). *The Time Trap, 4th Ed*. New York: Amacon.
[5] Menon, S. and Horney, C.L. (2008) Mobile Internet Device (MID) and Chip Market Opportunities. Strategies & Insight into the Emerging Class of Mobile Internet/Multimedia Devices. Report No. 8040. Forward Concepts (http://www.fwdconcepts.com/MID8.htm)
[6] Smith, B. (2008) ARM and Intel Battle over the Mobile Chip's Future. IEEE Computer Magazine, Vol 41, 15-18
[7] Vijayan J. (2008) Yet Another Laptop Theft: Agilent Warns 51,000 Workers of Potential Data Compromise, Computer World, March 2008.
[8] www.yubico.com