

# Balancing Privacy with Usefulness in Mobile Presence Solutions

Sara Lorien Smith  
Rensselaer Polytechnic Institute  
79 Forest Road, Felton CA 95018  
sara@got.net

## ABSTRACT

Mobile presence is a concept innovated by instant messaging applications, allowing users to display a status that demonstrates their availability and presumed willingness to communicate. As society becomes increasingly mobile, the need for more sophisticated presence systems has been identified. Unfortunately an increase in usefulness of such systems comes with a huge trade-off in terms of privacy. This paper will explore those trade-offs, examine user attitudes about privacy, and offer some design considerations for those interested in implementing more sophisticated presence models in their mobile products.

## Author Keywords

Presence, mobile communication, location, context-aware computing, privacy

## ACM Classification Keywords

H5.2 – User Interfaces

## Introduction

Mobile phones and more specifically smart phones that include voicemail, text messaging, and email have given users the ability to facilitate communication anytime, anywhere. For most users, this has been a mixed blessing. While the convenience factor of a mobile communication device is high, the trade-off is that the device demands our attention through notifications that somebody wants to communicate with us. The process of choosing if, when, and how to respond to a message forces a re-focus of our attention, at least for a short period of time. (1) Choosing to respond to the communication can further pull us away from a task. This can be distracting, and cause loss of productivity if the interruption is too frequent or unwelcomed.

Internet messaging programs have used the concept of presence for many years now to help manage this issue. Quite simply, users present a status that indicates their availability for communication. Typically this is done via icons that show a person as Available, Busy, Away, etc.

Some programs allow users to create customized statuses that could optionally include their specific whereabouts

(ie. Busy – At the Dentist). This system can be cumbersome. If the presence system requires manual updates to status, you must consciously take time from your day to modify your status. This is time lost from other activities.

Additionally, the standard presence model introduced by internet messaging assumes a flat hierarchy of relationships with others. When your status shows as available, you are available to everyone. Unfortunately communication doesn't follow these strict rules, especially in the business environment. Every time a request for communication is made, we must make a value judgment about the amount of attention to pay to the request as well as the speed at which we respond. Some systems allow users to create buddy lists with different displayed availability for different individuals or groups of people. This too is cumbersome and doesn't take into account the plethora of snap judgments that a person consciously or unconsciously makes when a request for communication is received. These judgments are largely unconscious, but may include factors such as the rank of the person contacting you, your like or dislike of the person, the perceived versus actual urgency, how much time the communication is likely to take and how much it will distract from your current activity, whether the person you're currently with would find it rude, and whether your current location is conducive to such a conversation.

As one can see, creating a rule set that effectively manages the zillions of possible scenarios would be near impossible. In an attempt to find a workable solution, many companies and universities have turned to the idea of having one's presence automatically derived from a number of methods. Some presence enabled systems already pull information from a person's calendar to determine their availability. The assumption is that if you are in a meeting or it is outside of business hours you are busy or unavailable. Otherwise, you are available. This is overly simplistic, and doesn't take into account all the possible exceptions. Perhaps your meeting only requires a smidgeon of your attention and you are available for IM. Or maybe your desire is to always be available to your wife or child regardless of what you are doing in case of emergency. Most current presence based systems assume black and

white rules when our day to day lives and relationships usually fall into an area of grey.

### **Next Generation Presence**

The solutions being proposed by companies and university researchers to combat all these challenges are starting to focus more and more on automated systems that determine presence based on other factors. Location and activity are being the most heavily explored. Your physical location could be tracked through GPS or GSM technologies tied to your mobile phone. It could also be tracked by sensors worn by an individual or via surveillance methods. Your activity could be shown by determining if you are on the phone or your computer, who (if anyone) you are currently communicating with, or even sensing your mood and pulse rate. Some activity indicators being explored are hard-coded to make certain assumptions. For example, if you are searching Craigslist, you are most likely not working and therefore available to who-ever wants to communicate with you. Other systems are intelligent and through trial and error, will learn your communication styles, who you prefer to communicate with, and who you generally avoid. (2) (3) (4)

### **Privacy**

While such technologies would certainly take the burden off the individual for managing their availability information and potentially minimize unwanted disruptions, they come with a huge value trade-off. In order to make use of such a system, one must sacrifice a level of personal privacy.

Privacy is a hot button topic in the digital age. People are becoming more and more concerned about how easy it is for others to learn their personal information via the internet and use it for unwanted solicitation or even fraud. The concerns about privacy don't end with the internet, however. People also worry about their phone calls being listened to, their email and text messages being read, being watched via video surveillance, location being tracked via satellite or other means, and many other issues brought forth by technology. This is in addition to traditional concerns about others obtaining personal information from snail mail, credit card and check transactions, and public records that maybe shouldn't be public.

But what exactly is privacy? It is a complex concept with no universally accepted definition. One of the most commonly used definitions was provided by Warren and Brandeis in 1890 (Brandeis later went on to the Supreme Court). Basically, privacy, they said, was the right to be let alone. (5) Malcolm Crompton expands the definition by saying that "privacy is part of the claim to personal autonomy" and that "some fundamental part of human dignity requires privacy". (6) Modern definitions often focus around the protection of information about one's self so that it doesn't fall into the hands of someone that might use such information to slander, defraud, or harm you.

It comes as a surprise to many Americans that privacy is not a specifically protected right in our constitution, when there is almost a universal desire to have it. Some countries including France do have clauses in their constitutions that protect this right and some state governments such as California do as well. Companies and government agencies may have privacy policies that spell out the rights or lack of for the individuals involved with them. But overall, there are no guarantees. This is why legal cases involving the issue of privacy are so complex and there is little consistency in the outcomes. (7)

### **Privacy Meets Presence**

So, we know that privacy is a big concern for most individuals, especially after it has been violated in some way. But just how touchy is the subject of privacy in terms of availability and presence? It turns out, quite a lot. A 2006 survey by Harris Interactive of 1000+ adult mobile phone users showed that only 56% of respondents would be comfortable with their spouse knowing their whereabouts via the use of presence services, 46% wanted their kids to know and 43% for other family members. Even more surprising is that only 6% said they'd be comfortable with a co-worker having access to their location via presence and 5% for the boss. (8) A more comprehensive though less scientific survey of over 38,000 adults conducted by MSNBC showed similar patterns and also demonstrated a high level of concern over others knowing what one is doing, and not just where they are doing it. (9)

A number of studies have been conducted that tested specific mobile presence solutions. In most cases, these studies focused on sharing location and availability information with people in your close social or family circle. In these circumstances, people were often less guarded about their privacy and willing to share this information with people for whom there was already a level of trust. Many reported greater feelings of connectedness with the others. This was especially true for couples who were physically separated from each other by great distances. (10) (11) (12) (13)

Based on the surveys of people's attitudes about location presence, however, it is a safe bet that these study results could not be duplicated if conducted with business associates, clients, or even strangers. If asked, most people are highly uncomfortable with the idea of their employers watching and tracking their every move through surveillance or reading their messages. And most are outraged at the idea that the government might be listening in on their cell phone conversations.

### **Presence Needs Within Various Constituencies**

What are some of the issues for the various parties involved in the debate about whether the benefits of

location and activity based presence outweigh the privacy issues involved?

Corporations want to maximize profits. A big part of this is managing employee productivity. An increase in technology has seen an increase in the number of distractions to workers. Some are voluntary by the worker, such as surfing the web when they should be working or claiming to be working from home using mobile technology when they are really at the beach. Other distractions are involuntary such as the mass amounts of email and frequent phone interruptions by clients or colleagues. Companies want more information about how their employees use their time, so that they can find ways to improve productivity and discipline or eliminate workers who abuse or misuse company time. Companies also want to ensure that its employees can be trusted and are not giving away secrets that could hurt the business. Presence based systems could provide this kind of information.

Additionally, corporations are concerned with protecting themselves from lawsuits. To this end, they want to be in compliance with whatever laws are in place with regards to privacy while still maintaining their own best interests.

The government has different goals. While individual offices probably have similar concerns about employee productivity and trust, the government has an even larger mission. They need to maintain public security and safety and a big part of this is keeping tabs on criminals, terrorists, spies, political figures, and other suspicious types. To be effective, a government must balance public confidence with the goals of achieving peace and prosperity both nationally and on a global scale. The United States government frequently comes under attack by its citizens for violating privacy in the interest of national security, but individual comfort with privacy violations is greatly influenced by national and international events. Immediately after September 11<sup>th</sup>, US citizens were much more willing to give up certain "rights" in the interest of catching terrorists. Prior to this event, there was a more closed mindset.

Governments are also concerned with ensuring that laws are abided by and taxes are paid so that the business side of government can continue to run. Presence based systems could be an important tool in keeping track of the people and activities that are a threat to the status quo.

Individuals usually understand and agree with the interests of corporations and government at a logical level, but not in practice. Why? Because to be effective, both government and corporations need to take away some rights to privacy in order to achieve their goals. On an individual level, people want to protect the financial, social, emotional, and physical security of themselves and

those close to them. This means safeguarding information that could make them victims of fraud, social ridicule, or discrimination, or that could place them in physical danger. Most people are also interested in protecting their image in the eyes of society and those in their personal life and network. Nobody wants to be caught in a lie and risk loss of credibility and trust. Individuals also hate being solicited to, and dislike marketers collecting and using information about them. Lastly, individuals want the security of knowing that certain rights are guaranteed to them by law and that they have an appropriate recourse if these rights are violated.

Individuals have both the most to gain, and the most to lose with the implementation of next generation presence technologies. On the one hand, it can help people to achieve a better work/life balance and better manage their time and productivity, both in their careers and personal lives. Having increased information about your children's activities and whereabouts can help you to protect them, and even to be a better parent. And knowing the activities and whereabouts of your friends and family can help you to empathize better with their day to day struggles and facilitate communication when others are most receptive to it. It can even improve your effectiveness as an employee.

Even with all these potential gains, there is a very high potential for abuse of this knowledge by other individuals, companies, and government. In the wrong hands, the knowledge of the whereabouts of your child through their cell phone could enable a kidnapper to more easily abduct your child. Knowledge of who you talk to, when, and for how long can make it easier to scam you. Somebody finding out and going public with the fact that you spend every Friday night at a sex club could ruin your public standing and your marriage. Your disability benefits could be revoked when your activities and locations don't coincide with your claimed ailment.

Some of these abuses may seem far fetched but the reality is that all this information about you would be stored somewhere. Presence based systems would detect and store information on various servers which could be accessed by those with the proper credentials or by hackers if security was weak. One might argue that the best security for such a system then is to only show current information about activity and location, and not store any history. Such a trade-off would probably meet the needs of individuals, but would not meet the needs of businesses and government, the ones who are probably funding the technologies in the first place.

### **Presence Design Considerations**

So given all of these issues, what is the answer? Should we hold on to our simple, though ineffective presence model initiated by IM technologies? What design considerations should be included to minimize the potential for abuse and

maximize the usefulness of having activity and location information about others?

First, any person who uses any presence based service, whether voluntarily or as mandated by an employer, should have full access to their history file. A person should be able to see what information is being recorded about them, and who has accessed it. I'd compare it to an individual's rights with credit reports, where a person may challenge the information that is included, see who has requested their information, and when. Unlike credit reports, this information should be free and accessible as often as is desired. Parents/guardians should have full access to information about their minor children until they come of legal age. The servers that store this information should have the highest level of encryption and strict access requirements.

Second, individuals should have the option of turning off activity and/or location tracking on their communication devices while still being able to communicate via phone, IM, etc. Outside of work hours, employers have no right to monitor the activities of their employees. Individuals will of course have to weigh the benefits of keeping this on or turning it off against their personal needs, but it should always be an option.

Third, people should have the option of allowing some persons to see their activity and location presence while denying this information to others. As discussed earlier, there is no one-size fits all when it comes to communication and relationships. Though this may be a tedious step as it would have to be done manually, end users will appreciate having the option for control even if they opt to not use it.

Last, companies and governments must create policies and/or laws regarding how presence information will be used, and what an individual's rights are in terms of the technology and data collected. People need to be educated on the issues and have a clear recourse if their rights are violated. The message needs to be sent from the very beginning that abuse will not be tolerated.

Only when all of these areas are covered, can people be comfortable with location based presence technology and feel that the benefits outweigh the reduction in their personal privacy.

### **Bibliography**

1. McCrickard, D. and Chewar, C.M. (2003) Attuning notification design to user goals and attention costs. *Communications of the ACM*, Vol. 46. March 2003. pp. 67-73.
2. Maglio, P. P., Barrett, R., Campbell, C. S., & Selker, T. (2000). *Suitor: An attentive information system*. Proceedings of the International Conference on Intelligent User Interfaces 2000 (IUI 2000). New York: ACM Press, pp. 169-176.
3. ter Hofte, G. H., Mulder, I., Grootveld, M., and Slagter, R. (2002) Exploring a design space for place-based presence. In *Proceedings of the 4th international Conference on Collaborative Virtual Environments* (Bonn, Germany, September 30 - October 02, 2002). *CVE '02*. ACM Press, New York, NY, 151-152.
4. Peddemors, A. J., Lankhorst, M. M., and Heer, J. d. (2003) Presence, Location, and Instant Messaging in a Context-Aware Application Framework. In *Proceedings of the 4th international Conference on Mobile Data Management* (January 21 - 24, 2003). M. Chen, P. K. Chrysanthis, M. Sloman, and A. B. Zaslavsky, Eds. *Lecture Notes In Computer Science*, vol. 2574. Springer-Verlag, London, 325-330.
5. Warren and Brandeis (1890) The right to privacy. *Harvard Law Review*, vol. IV. December 15, 1890. Retrieved from: [http://www.lawrence.edu/fast/boardmaw/Privacy\\_brand\\_warr2.html](http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html) on October 21, 2007.
6. Crompton, Malcom, Federal Privacy Commissioner (2001) What is privacy? In *Privacy and Security in the Information Age Conference*, 16-17 August, 2001. Melbourne. Retrieved from: <http://www.privacy.gov.au/news/speeches/sp51note1.html> on October 21, 2007.
7. Vogt, Carlton. (2007). Privacy: An important but complex right. *Infoworld – Ethics Matters*. Retrieved from: <http://www.infoworld.com/articles/op/xml/02/03/08/020308opethics.html> on October 22, 2007.
8. Harris Interactive (2007) Location-based services and presence technology: the future of telecommunications in closer than you think. *The Harris Report*, Vol. 2, Issue 1. February, 2007. Retrieved from: [http://www.harrisinteractive.com/news/newsletters/HarrisReport/HI\\_TheHarrisReport\\_2007\\_v02\\_i01.pdf](http://www.harrisinteractive.com/news/newsletters/HarrisReport/HI_TheHarrisReport_2007_v02_i01.pdf) on October 19, 2007.
9. MSNBC. (2007) Is your privacy important? Are you losing it? *MSNBC – Technology and Science*. Retrieved from: <http://www.msnbc.msn.com/id/14850268/> on October 22, 2007.
10. Brotman Karmin, L. S., Seligmann, D. D., Sammon, M., and Peebles, E. (2007). Evolution of a concept: from technology to end-user to enterprise. In *CHI '07 Extended Abstracts on Human Factors in Computing Systems* (San Jose, CA, USA, April 28 - May 03, 2007). *CHI '07*. ACM Press, New York, NY, 1765-1770.
11. Bentley, F. and Metcalf, C. (2007) Sharing motion information with close family and friends, In *CHI '07 Extended Abstracts on Human Factors in Computing Systems* (San Jose, CA, USA, April 28 - May 03,

- 2007). CHI '07. ACM Press, New York, NY, 1361-1370.
12. Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., and Powledge, P. (2005) Location disclosure to social relations: why, when, & what people want to share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Portland, Oregon, USA, April 02 - 07, 2005). CHI '05. ACM Press, New York, NY, 81-90.
  13. Dey, A. K. and de Guzman, E. (2006) From awareness to connectedness: the design and deployment of presence displays. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Montréal, Québec, Canada, April 22 - 27, 2006). R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, and G. Olson, Eds. CHI '06. ACM Press, New York, NY, 899-908.