Tutorial on Privacy and Wearable Computing

Instructor: Thad Starner (Georgia Tech)

"Those who design systems which handle personal information therefore have a special duty: They must not design systems which unnecessarily require, induce, persuade, or coerce individuals into giving up personal privacy in order to avail themselves of the benefits of the system being designed."

These words, written by Leonard Foner in his PhD thesis, seem especially applicable to wearable computers, which may become storehouses of users' most intimate information. Indeed, designers of early ubiquitous computing systems often cite privacy as one of the key concerns of users in adopting their technology. Privacy concerns are not equivalent to security concerns. Security involves the protection of information from unauthorized users; privacy is the right of individuals to control the collection and use of personal information about themselves.

When considering privacy in system design, one must consider what threats the system might face. This problem is often difficult and must be put in the context of the desired functionality, location, owner, safeguards, and user perception. For example, a radio frequency identification card used to track employees at a public university may be effective for security, but it also raises privacy concerns. Could the university use the system to "spy" on its employees or students? Could an estranged spouse use the system for harassment? Is the data subject to court subpoena or the "Freedom of Information Acts" being initiated by various governments? Could it be used to prove a defendant's presence at a particular location in a civil or criminal case? Or, more indirectly, could the logging data be used by recruiters to determine which students spend the most time in the laboratories or on campus? Who decides what data is revealed to whom and what safeguards must be in place before the data is released?

This tutorial will frame such questions in a historical context and attempt to enumerate the risks and safeguards that can be addressed by wearable computing. Specific wearable and ubiquitous computing systems will be examined. Participants will be part of an ongoing effort to lend structure to a socio-technological approach to privacy in the field.

Outline of Tutorial Content

- Historical perspective
    - Definitions
    - Is privacy purely a modern concept?
    - Role in England and the United States
- Common reactions to privacy advocacy
- Modern politics, mishaps, and use in advertising
- Legislation, regulation, and investigation
- Privacy as big business
- Affect of privacy in adoption of ubiquitous computing devices
- A modern system-builder's perspective
- Approaches to preserving privacy
    - Physical
    - Technological
    - Legislative
    - Social
    - Obscuration
- Guidelines and resources for wearable and ubiquitous computing
- Case studies

Instructor: Thad Starner

Thad Starner graduated from MIT in 1991 with Bachelor of Science degrees in Computer Science and Brain and Cognitive Science. He joined the Speech Systems Group at BBN as an Associate Scientist. Starner was named a United States Air Force Laboratory Graduate Fellow and returned to the MIT Media Laboratory where he earned his Masters and Doctorate in 1995 and 1999, respectively. In 1999, Thad joined Georgia Tech's College of Computing as an Assistant Professor. He is a founding member of the MIT Wearable Computing Project and the IEEE Wearable Information Systems Technical Committee. Starner co-founded the IEEE International Symposium on Wearable Computers (ISWC) and has served as the general chair and on the program committee. Thad's current work researches the use of computational agents for everyday-use wearable computers as a segue to artificial intelligence.