Challenges for Privacy with Ubiquitous Sensor Logging

James Scott

Microsoft Research Cambridge
jws@microsoft.com

Abstract. In this position paper I discuss some implications for privacy of a future where sensing and logging of sensor data is ubiquitous.

1 Ubiquitous Sensing: A Genie Awakened

Sensors are ubiquitous. To take the medium of sound as an example, the number of microphones present in a home, office, or even in public spaces like streets is huge and is expected to keep growing. These sensors are not just present in situated hardware such as telephones, computer terminals, etc, but are also present in mobile devices such as phones, media players (e.g. iPods), consumer electronics such as navigation devices, and so on. The deployed sensors are also not under a single entity's control, with individuals, corporations and governments all having control over many sensors.

While audio is perhaps the most pervasive sensor type (due to telephones), other types of sensors deployed and being deployed include cameras (phones, CCTV, webcams), location sensors (GPS, radio-based), environmental sensors, physiological sensors, neighbourhood object/person sensors (RFID, radio-based), etc.

2 Ubiquitous Logging: A Giant Stirring?

Automatic logging (as opposed to deliberate, manually triggered data capture) is not yet ubiquitous. While personal logging devices such as SenseCam [1] and Personal Audio Loop [2] have been developed, such automatic logging is not found in commonly deployed devices. However, this is not because the sensing or logging technology has proven immature. Instead, the reasons for a lack of deployment are because of the difficulty of managing the data, and the lack of applications which can make use of such data. In terms of data management, while software such as MyLifeBits [3] has been developed, such software is not widely available and there still remains significant difficulty for users in managing their personal media. As such, deployed end user applications using logged rather than realtime data are still predominantly focused on simple finding and replaying media for personal entertainment. Applications which can usefully manage and navigate large sets of data items are being explored in research environments, such as in health monitoring (e.g. show my doctor a picture of every meal I've eaten in the last month).

3 Privacy Issues in a Brave New World

Let us jump into the not-too-distant future when sensors are even more pervasive, storage capacity is essentially infinite, computation to data mine and search sensor data is plentiful, and networking is fast and cheap. Furthermore let us assume that applications have arisen which have convinced users, corporations and governments to log sensor data (images, sounds, physiological data, etc). In this world, any sensor might be logged by default rather than only logged in specific circumstances.

What are the challenges to privacy in such environments? The security of data on one's own devices is not necessarily the main source of threats to privacy. Much more of an issue are data logged by others. With pervasive logging, everything one does or says may be recorded and made public or shared with interested third parties.

There is no single panacea for this issue; solutions may come from many domains, including but not limited to:

Legal – existing laws in some countries concerning "data protection" can be used, rewritten, or better enforced. This may prove easier to accomplish against corporations than individuals or governments.

Social – social etiquette and taboo may make the publication of data that others would consider private very distasteful, and the threat of retaliation in kind for such offenders might keep the effects minimal.

Technological – Proactive jamming or obfuscating equipment may be used on a large scale, e.g. camera-lens detectors or GPS signal jammers, may become more widespread. However, it may be illegal or very difficult to jam many sensors effectively. Alternatively, automated tools may help users keep track of their information "footprint" so they can more easily send removal requests reactively.

Virtual – personal spaces such as homes may become more important for privacy as a haven away from pervasive sensing. One possibility is that the nature of interacting via a virtual medium may become more compelling since it is easier to control the "signal" that one presents to the world. Indeed, security research has identified ways of creating channels which mimic many (unlogged) real world conversations, e.g. the ability to anonymously participate in situations even as complex as financial transactions [4].

To conclude, ubiquitous sensing's impact on privacy poses social, technical and other types of challenge, making this an interesting area for future research.

References

[1] S. Hodges et al., "SenseCam: a Retrospective Memory Aid". In Proc. UbiComp 2006, Springer.

[2] G. Hayes et al., "The Personal Audio Loop: Designing a Ubiquitous Audio-Based Memory Aid". In Proc. MobileHCI 2004, ACM.

[3] J. Gemmell et al., "Passive Capture and Ensuing Issues for a Personal Lifetime Store". In Proc. CARPE 2004, ACM.

[4] F. Stajano and R. Anderson, "The Cocaine Auction Protocol: On the Power of Anonymous Broadcast". In Proc. Workshop on Information Hiding, 1999, Springer.