

## **Privacy and wireless sensor networks**

Lesley Hanna, Stephen Hailes, University College London

Wireless sensor network technology has the potential to change the way we live work and do business, with applications in entertainment, travel, retail, industry, medicine, care of the very young and very old, disaster and emergency management and a host of other areas. There is the potential to enrich lives and make processes easier. However, there are some potentially negative aspects of the formation of these networks, and one of them is the prospective loss of privacy of the individual.

There are a number of possible definitions of privacy, but for the purposes of this article we will select 'informational self-determination' since it is the information which is produced from the data generated by sensors and other devices in the networks which has the potential to threaten our privacy if misused or mishandled.

### **Public perceptions of privacy**

The quotation 'Privacy is dead – deal with it' was attributed to Scott McNealy the CEO of Sun Microsystems back in 1999. This must have been at least in part a response to the apparent readiness with which people will part with personal information in return for a real or perceived advantage without understanding the implications of their actions. The example most often used to illustrate this is loyalty card schemes which show that in return for a modest discount, people will part with information which spans spending, health, location, consumption and behavioural habits. The data generated belongs to the card issuing authority which can do what it likes with it since it has been obtained legally and with consent of the card holder. This begs the question as to whether users and suppliers of wireless sensor networks truly need to be concerned about privacy at all.

The technology represented by these networks is non-obvious to most people. They do not understand it and therefore may not be in a position to make balanced judgements concerning the extent to which it may have a negative impact on their own standards of privacy. The potential for improvement in quality of life offered by the technology is huge, but autonomy and reconfiguration may obscure both the data and the use that is made of it. Lack of interfaces makes it difficult to review data and it may not be possible to show where the data came from. The average person is not in control of the technologies applied to them. Even more, it is not clear who will decide what technology is used and where and how it will be used.

Many people appear to believe that if they have nothing to hide then they have nothing to fear from new technologies. This is a rather naïve viewpoint, since there is information which all of us may prefer not to be generally available. Without appropriate privacy safeguards the information may go into the public domain straight away, which is

potentially undesirable for a number of reasons. Early stage pregnancy, the details of certain medical conditions, or information on our recent spending may be made freely available to our close relations and friends but is not appropriate for general consumption. The public need to be informed what technology can do in general, told of specific instances when technology is deployed which might affect them, and educated about what might be done with the data.

In the last 2-3 years there has been a rise in interest in privacy issues, stimulated by the widespread introduction of radio frequency identification (RFID) technology. RFID gives quite low-level intrusion into privacy which is the same level as much data of the data from wireless sensor networks. Coupled with this, however, we are also seeing a change to our culture towards keeping ever larger quantities of data for longer and longer periods of time. Also, data tend to be shared unless there is a reason not to do so. Analysis of even low-level data can yield a surprisingly large amount of information on an individual. Deployment of wireless sensor networks imply the collection of enormous quantities of mostly low-level data which if retained and analysed would provide information which could seriously compromise individual privacy.

Another driver, apparently working contrary to the maintenance of privacy, is that homeland security and anti-terrorist activity means that people are prepared to compromise on their own privacy in order to identify potential terrorists and other criminals. However, the collection of ever larger amounts of data can result in increased problems in identifying particular traits making the task harder.

It is clear that there is a need for a balance between the interests of the public and those bodies who wish to have access to data generated for whatever reason. This balance is very difficult to assess and needs informed debate to reach a consensus.

## **Application areas for wireless sensor networks**

About 8 billion embedded computers are sold every year. Embedded computers are dedicated computing power found in a wide variety of devices. Although at this point in time very few are networked, this figure gives an insight into the potential scale for implementation of reconfigurable wireless networks. A study by IDC estimated that in 2012 the installed base of networked computers would be over a billion units. Handheld, entertainment and industrial or automotive devices would raise this figure to 6 billion, rising to 16 billion when appliances and toy devices are added in. Once RFID sensors and tags are added the figure exceeds 1 trillion<sup>1</sup>.

Looking at just a few examples of application areas for wireless sensor networks:

The average age of the UK population is rising with a consequent strain on health service resources. Equipping the elderly or vulnerable with simple, wearable devices which will monitor health and automatically report and summon help if there is cause for concern, can enable such people to remain in their own homes safely, avoiding institutional care and reducing the need for constant professional attention. Such things as heart rate, blood pressure or blood sugar levels might be transmitted regularly as part of the data generated by a body area network (BAN). For a very elderly or cognitively impaired person, however, it will also be important to ensure that they are able to look

---

<sup>1</sup> Vernon Turner, 'Sun's Throughput Computing Strategy to Create a Quantum Change in Server Performance' Feb 2004 available from [www.sun.com/processors/whitepapers/idc\\_whitepaper.pdf](http://www.sun.com/processors/whitepapers/idc_whitepaper.pdf)

after themselves properly, so data will be recorded on activities such as whether kitchen appliances are used, and use of bathroom facilities. People will be less willing to have data on their personal habits made available than on their heart rate, for example.

In commercial buildings and domestic dwellings, linking controls (eg thermostat, lights, ventilation) and appliances can offer major savings in energy efficiency as well as improved security, safety and convenience. The data collected by these 'smart buildings' will span security, safety, personal data and habits in order to carry out the building management tasks. This has privacy implications since access to the data will reveal information on personal habits. Even the wireless meter reading data generated by one of the major wireless sensor network applications currently used, could be useful to potential burglars.

When emergencies or disasters have occurred, linking together the data from all the information sources which survive the episode can protect emergency workers by improving information about what conditions they face, help locate and treat casualties, assist evacuation and aid remediation. However, obtaining some of the data may infringe the normal privacy expectations of the individual. Given that a person trapped in the wreckage of their crashed car is likely to be entirely happy to release any personal data to assist the emergency services in saving them, but is not likely to be in a position to indicate that fact, it will be necessary to establish rules and guidelines under which normal privacy expectations may be waived. The crashed car example is straightforward, but what of the occupants of adjacent vehicles which have not been a part of the incident, but whose information may be taken and used? Ad hoc networks which are self-configuring and will reorganise as devices fail or are destroyed or are added, are much more difficult to control.

The project SWAMI: Safeguards in a World of Ambient Intelligence (<http://swami.jrc.es>) has deliberately looked at what the consortium calls 'dark' scenarios. These dark scenarios review potential negative aspects of ambient intelligence including privacy issues.

## **Consent versus consensus**

Privacy is commonly dealt with by using the principle of consent. In order to purchase or participate consumers are required to consent to their data being used in particular ways. There are laws to limit how data may be used or supplied to third parties, but data protection and privacy are not the same thing. Generally, if the general public do not like a particular technology they will make their opinions clear by using or sourcing alternatives. In the case of ubiquitous sensing this is not a viable alternative. Safety-based systems or mandatory ones such as road-user charging do not permit opting out.

The information available from the data produced by sensor networks can be non-obvious. It is also not necessarily clear what data are being captured, and the data which are being captured are not necessarily under our control. Informed consent may not be possible, rather we may move towards a consensus. Even this consensus may be challenging to achieve, especially since the privacy expectations of different communities or countries seem to vary. What is clear is that wide-scale use of wireless sensor network technology is likely to change us as a society. If people are concerned about their privacy it will result in a change to their behaviour but the social implications are not yet clear.

One way forward is to hold the government or other authority which has control of the data accountable for the uses to which it is put. Governments in particular are capable of thinking up new uses for data which were never covered in the original design brief. To some extent companies will be cautious of their reputations and therefore unwilling to alienate customers who can choose alternative service providers elsewhere.

### **Use of data**

We seem to be keeping a lot more data generally than we did ten or even five years ago. One of the reasons for this is likely to be the relative ease and cheapness of storing that data. Data retention does not seem to be a particularly high-profile issue within Europe, but it certainly is a rising subject for debate in the US. In June 2005 the US Department of Justice started to propose mandatory data retention rules for internet traffic. This was prompted by a high-profile child pornography case, but the proposed law was not restricted to this application. In Europe a law was passed by the European Parliament in December 2005 forcing phone companies and Internet Service Providers to keep details of their customers' communications for up to two years. Although there was initially a lively discussion, the subject no longer seems to be of general interest.

There are a number of reasons proposed as to why this type of data retention is inappropriate. Opponents have claimed that the times are too long and there have been arguments about who is responsible and who will pay for the 'data warehouses' required for storage. In addition using current systems it is relatively easy to mislead the system, assuming different identities, framing other people or even turning off systems. This leads to the risk that only ad hoc criminals or those who do not care will be caught.

Some applications of wireless sensor networks will involve a supply chain. When this occurs it is less clear where responsibility for maintaining privacy resides and there is a risk of people having expectations of other members of the chain or making assumptions which are not met. If the trend for keeping large amounts of data continues then data mining will become more automated. This has implications for the uses to which data may be put and also for the extent to which appropriate quality control may be imposed.

### **Addressing privacy issues**

If the issues associated with privacy are not honestly debated in a reasoned and open way there is a risk that there will be a public backlash which will result in mistrust and consequently the technology will not be used for the many valuable applications where it can provide significant benefit. The start of this process can already be seen in some of the attitudes to RFID technology where the potential for the technology in a multitude of uses is clear, but the limitations are less visible to the average person, resulting in mistrust and misunderstanding. Education of the general public is therefore a vitally important part of gaining acceptance for the technologies associated not only with wireless sensor networks but also others such as RFID and location-based services

For privacy protection to be given the importance which it will certainly eventually be accorded, it must be engineered into products at the design stage, not imposed post-hoc. There is no external incentive to do this now. Systems that protect our children and other vulnerable people and prevent our homes from being burgled must be safe from

malicious intent. There are also other privacy-enhancing technologies including security solutions which can be used to limit invasion of privacy.

We can also ensure that we limit collection of data to that which is required to carry out the desired function and nothing else. Identity data can be discarded or coarsened to the maximum extent to still allow the desired information to be generated. Specific users should not be identified unless there is a need. Only a subset of the identity may be needed.

The lack of mandatory requirements arising from a legal framework means that guidelines must be developed within technology communities. Although external legislation may be more desirable, regulations developed by a group of users can be very effective, especially if there are penalties which can be imposed for non-compliance. Single authorities which are self-regulating, such as government departments or agencies, are rather less attractive as a prospect. One potential method of assessing the impact on privacy of a specific application is by the use of 'privacy impact assessments' carried out by trained personnel with a good understanding of privacy.

The areas where public privacy concerns are likely to be generated first are in transport systems and in medical applications. Any citizen should be able to understand what uses will be made of data about them for example who can find out the data from their health monitoring equipment - their doctor, hospital, insurance company, employer, parent or child? Road charging schemes are likely to be a common use of large-scale sensor networks. Will that data be used to identify speeding vehicles which are then reported to the police? Can an employer access data on a company vehicle he owns in order to ensure that employees driving them are making the best use of company resources?

Since the average person may not be able or willing to try to understand the full implications of deployment of a technology, it may be appropriate to have a body which represents the consumer or citizen where the members are skilled and experienced in the technology but not affiliated to any of the stakeholders. Perhaps that trusted body might also be responsible for privacy impact assessments as suggested previously. It may be, however, that privacy impact assessments have limited value if the full potential of any complex system will only become clear after deployment.

A clear legal framework will be required to control invasions of personal and corporate privacy. This legislation must be fit for purpose, addressing both current technology and accommodating those which are still being developed. Laws covering a particular technology are unlikely to be successful. Work is still required on what form the legislation should take, for example whether there should be restrictions on what data may be collected, mandatory security or limitations to data access. Certainly it seems likely that it should be possible to discover who has been able to access aggregated data. There must also be clear and appropriate punishments for infringement.

## **Conclusion**

Wireless sensor network technology has a tremendous potential to enhance quality of life and is likely to be widely used in the medium-term future. However, inappropriate use of the data generated may have a negative impact on privacy which could limit use of a technology which has significant potential for good. Improving awareness, protection of

the individual through a combination of legal requirements and industry best practise, and consideration of privacy issues at the product design stage should help to protect personal privacy and assist more widespread use of a powerful and beneficial technology.

### **Acknowledgement**

The RUNES (Reconfigurable Ubiquitous Networked Embedded Systems) project aims to enable the creation of large-scale, widely-distributed heterogeneous networked embedded systems that interoperate and adapt to their environments. It is funded by the European Commission and is composed of 21 partners from 9 countries. As part of the work undertaken, RUNES researchers have identified the major barriers to uptake of the technology, one of which is privacy. The RUNES project is funded by the European Commission (contract IST-004536).

Some of the information and views contained in this article were captured at 'A Fine Balance', a multi-disciplinary, international event which took place in November 2006 in London. The event was organised with the aim of bringing together experts on the impact of sensor network, pervasive computing and location-based technologies on privacy and to discuss the issues and how they might be addressed. The contribution of many experts in this field is gratefully acknowledged.