

Consultation on the early challenges regarding the "Internet of Things"

<http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=IoTconsultation>

eNACSO reply:

Society faces major challenges in relation to how we manage the roll out of a range of new technologies which are capable of collecting, storing and transmitting substantial amounts of information about the physical whereabouts of individuals or objects i.e. unlike the highly variable location data which is generated through mobile phone networks, the new generation of devices work with a very high level of accuracy and can give quite precise geographical details of where a person or an object is right now, or where it or they have been in the past. "The past" could be a matter of minutes or hours ago, or days ago or even longer.

As the Report notes, RFID is one such technology which is already in widespread use. RFID and similar technologies are important not least because, typically, they are capable of being produced extremely cheaply and distributed on an enormous scale. In addition, at least in the case of RFID, precisely because the device is so small and potentially unobtrusive it could very easily be attached to an item that is, in turn, tied to a particular individual e.g. via a garment or a school satchel.

The major growth of RFID has been driven by industry's search for improved systems of tracking and controlling stock levels e.g. in shops and warehouses but, as the Report again notes, analogous or similar technologies are also coming on to the market for use elsewhere e.g. within the UK all new passports contain a small, thin radio chip which holds personal information about the carrier. This chip can be read remotely without the necessity for any physical contact between the passport document and a chip reader. There are also several other "contactless" systems already in use or being developed which, again, contain a range of personal data. e.g. London Transport's "Oyster" card. Admittedly, RFID and similar technologies at the moment have a very short range but it is highly likely that the range of some of these systems will increase. As the range increases so the potential for unauthorised interception of the data also increases. Not all of these systems choose to use encrypted personal data, or if they do the level of encryption may not be the strongest.

The civil liberties implications of the development of technologies such as these hardly need to be rehearsed but, clearly, there will be legitimate concerns about the extent to which arms of the state e.g. the police or security services, can access and use location data. Importantly there are also major concerns about how different commercial entities might collect and use location data. Potentially this kind of data could be of great economic significance, allowing companies, for example, to serve advertisements to people based on their known current geographical location or patterns of travel.

In the child protection space in the UK we have already had to face issues about the security of location data. Here a number of companies started to market child location services using location data supplied via the mobile phone networks. There was a concern that unless sufficiently stringent security checks were put in place an unauthorized person with bad intentions could locate and track a child. Alternatively in situations where, for example, a couple had broken up following instances of domestic violence, it is not uncommon for the violent partner to be barred from any contact with the children, or to be allowed contact only in controlled or supervised circumstances. A great deal of effort might have been invested in creating new identities for the partner and children who were victims of the violence, including establishing a new home at an address unknown to the violent partner. Unless properly thought through, the security of that new address can be destroyed with the click of a mouse, thereby

putting both the adult partner and the child or children in perhaps very serious danger.

Following substantial negotiations a code of practice on the security aspects and the marketing of child location services was adopted by the UK industry and, as far as we are aware, it has worked broadly satisfactorily. However, at the time the code was agreed there was not a single mobile phone available in the UK consumer market that had a GPS module built in. GPS based services were therefore not covered by the code. GPS is a satellite based technology that works entirely independently of the mobile phone networks. Today a huge proportion of the new mobile phone handsets include a GPS module as standard. Whilst handset-based GPS is still a one way system, when linked to the capabilities of the mobile phone network and the internet it has the potential to become, in effect, a two way system with greatly enhanced power and capabilities.

In response to this new scenario, and in an attempt to bring GPS and RFID within a regulatory framework similar to that which the mobile phone networks had voluntarily entered into, in 2006 we worked with UK Parliamentarians to promote a Private Member's Bill to establish a licensing regime for any company or entity that wished to provide location based services ("Licensing of Child Location Services Bill, 2006", sponsored by Judy Mallaber MP). The intention behind this Bill was to create a system that would ensure the highest possible standards of data privacy and security for any location services which were specifically targeted at or related to legal minors.

At the same time as the child location services started to be marketed we became aware that mobile phone based devices were also being developed to be used, essentially, as surveillance devices e.g. with a capacity to be silently and unobtrusively converted either into remote listening devices, remote cameras, or both. Apart from raising fairly obviously child protection issues, this use of the technology seems to be insidious in almost any context.

A number of services appear to be in development which utilise geographical or location information that has been obtained from mobile phone based devices, utilising data obtained via wifi networks, GPS, the phone network itself, or a combination of these see: <http://mashable.com/2008/06/09/sense-network>. Note in particular that this company says it "...has set out togive (you) a visual map of your customers, letting you know where they are at a given point in time." See also <http://googlemobile.blogspot.com/2008/06/google-enables-location-aware.html>. Here, in a section headed "Google enables Location-aware Applications for 3rd Party Developers", Google says: "At Google we're very excited about the promise of location technology to drive innovation in the mobile industry. We of course use this location technology already in Google Maps for mobile with the My Location feature. However, we wanted 3rd party developers to also have access to the same location technology across multiple platforms."

In no sense do we wish to object to the development of location based technologies. Not at all. It is not hard to imagine many very useful and fun applications. But, to conclude, there clearly is a legitimate and widely-held fear that technology is, once again, starting to outstrip the ability of regulators and Governments to understand the public policy implications of its emergence. Just because something is technically possible, is not necessarily a reason to accept it is inevitable, much less that it is desirable or that it should be welcomed and allowed to operate free of any constraints. This area is uniquely important because it opens up the possibility of allowing very large databases to be created, of a kind which have never existed before, holding vast amounts of information about perhaps quite private aspects of our lives, not just which bus route we follow most days of the week.

For that reason we believe the Commission ought to initiate a wide ranging public debate about how we foresee location data being collected and used, both by commercial and public sector entities. We should not allow ourselves to sleepwalk into a surveillance society."

---OOO---

November, 2008