

Ambient Intelligence and the Limits of Privacy?

I speak today, not as someone strictly with a legal background, but rather originating disciplinarily in Social Policy and Ethics.

I find this stimulating though, as my topic will address each of these in questioning what types of laws do we require, which ones may possibly be ineffectual, what wider social and public policies may be necessary and what might be the ethical (as well as other challenges) that appear to be engendered by particular developments in Information and Communication Technologies.

It is clear that a number of technologies are on the horizon, and even more Beyond the Horizon, that have ramifications for society.

However, I wish to stress that what I am proposing is not the apparent neutral observation that technology springs into being and we must contend with the impacts on society, on policy, on law.

I will try to highlight how, at least within these ICT futures, the process of technological and scientific research is heavily embedded, interdependent and reliant on what can be seen as obviously social processes.

This can be in a purely marketing sense, such as for example Philips terming its labs, *Experience Labs*, where the idea is to sample and collect data on the human 'experiences' with and of technology.

However, I believe this to be merely just the surface, as a deeper reading and analysis of documents, conference proceedings, articles, etc., reveals both a keen desire to learn from the social (and its sciences) and open up space and dialogue for discussion on the potential futures that are on the horizon.

Roboticists for example aim to learn from the social to create more believable robots, engineers are exploring and highlighting their own view of the ethical issues at stake, and some scientists, such as Kevin Warwick, appear intent on pushing and challenging the boundaries of even philosophical questions as to the meaning of being human.

I state this, both to highlight the fact that the technology research process at least in much of ICT research is inherently social, and even more critically, I have found, and perhaps my other colleagues on the ICTethics project will agree or disagree, that there is an appetite for dialogue on the scientific, engineering and in other ways related sides, for exploring potential issues, risks and challenges that might be foreseeable in relation to technological developments.

As such, I strongly believe that there are issues, but I also, reflecting my background in social policy, believe that we as commentators and analysts can have a significant impact on these developments 'before they happen!' which in

any case I think is always a more preferable place to conduct analysis rather than scrabbling after the fact.

So, on the topic of this talk. Well I think it would be prudent to explore just what is meant by Ambient Intelligence, I think also it will be necessary to discuss some meanings of Privacy (although not too long or extended as we could easily have two whole conferences to do this).

On the most simplest level, as my colleague Prof. Steendam has pointed out is a set of technological developments that will enable our environments to become responsive, flexible and interpretative in relation to our needs, preferences, demands—even as the engineers suggest, pro-sponsive. [see ISTAG reports]

A key aspect of the proposed set of technologies here is also that they will be unobtrusive, so for example new developments may see our needs and demands not even being communicated orally, such as is the case with developments in soft or 2nd generation biometric technologies.

What then is the Privacy Challenge? There are a number of ways to approach this.

We can express the fear that the type of networks and vast range of devices inherent in an Ambient Intelligence environment will mean an unparalleled amount of devices and places where we can be monitored, recorded and stored.

While there is a clear commercial drive, focused as well on end-user needs, the potential for abuse, even if we do not slip into 1984-esque worries, is certainly there.

I think in this regard, companies are already aware of the potential issues, although the regulatory wherewithal to regulate abuses would appear to be lagging behind.

A second way in which to see the challenge to privacy is linked to the idea emerging in Ambient Intelligence scenarios which is termed Social Intelligence.

At heart, the idea is related to the fact that a core feature of Ambient Intelligent environments will be the relinquishing of human control to machines.

These will in fact be making decisions and choices for us, based on past habit, based on stored preferences and reacting to behavioural or biometric characteristics.

Considering this then it is a distinct possibility that machines will be sharing and storing data, perhaps independent of any larger network (for example rooms in your house may be where certain data is stored).

The premise of machines and networks displaying social intelligence is that they will in fact aim to make decisions on sharing data within the strictures of what is socially acceptable. [use the example given by Phillips]

Clearly a number of issues can be seen.

Firstly we can see that in such scenarios informed consent would appear to be replaced by presumed consent.

It is unclear for example how one might be able to opt out of ambient intelligence environment in retail. The second is that such dispersed and pervasive networks would appear to present difficulties in terms of data traceability, data will have high linkability and perhaps be stored in a wide variety of places. Finally there is the issue of machines acting autonomously for us (and as such making use of data on us in proactive as well as reactive ways).

What is the meaning of the Privacy being challenged? The most obvious point to draw on here is the fact that given some of the features of Ambient Intelligence, and supposed ways in which they will operate, it would appear that current data protection legislation will either cause or encounter difficulties.

I do want to note, however, that data protection may not equate to what is defined as Privacy, I think its reasonable to suggest that data protection is clearly concerned with Informational Privacy but we can assume that there are other conceptualisations of privacy that we could use.

To examine data protection as outlined in directives then.

Firstly, it is difficult to see where consent to having my data recorded and stored can be built into pervasive ambient intelligence environments. Soft biometric devices and other sensors may not even be recording or storing actual personally identifiable data, but may provide other sensors and machines with the fact that I am male, or female, too hot, too cold, etc.

It is difficult as well to see how, within many ambient intelligence environments, knowing the purposes to which my data will be used can be sufficiently covered. Interpretative and responsive environments would appear to be a dynamic system where not all purposes can be expressed.

This leads onto another observation in that the definition of 'data controller' may likewise encounter problems, will data controllers be these autonomous decision-making machines?, the companies, the individuals themselves. What if a machine or network is only a data controller in relation to that individual for a short period of time?

I concede that each of these points can be addressed however. Clearly it would require perhaps another directive focused solely on some of the issues arising out of ambient intelligent environments.

Indeed we can see a pattern in data protection, and the protection of privacy in general, of the law responding to new technological developments which are seen as privacy threatening.

As such it may be reasonable to assume that the existing frameworks can be adapted, although my own feeling is that this may not be as easy as it could appear to be.

Is Privacy challenged in the eyes of all? This question leads me onto my final set of points, which is that while data protection has been a success, although this might need to be qualified.

It is unclear that people even currently place a high value on their own personal privacy, at least in the narrow terms in which it is set out in directives.

I think we can look to a number of studies, for example the work of Alessandro Acquisti suggesting a very low monetary value being placed on Privacy.

Developments here have seen increasing calls for Privacy Enhancing Technologies, but it appears to me that some of the rhetoric here is to automate the business of data protection and introduce technologies to solve the perceived problems created by other sets of technologies.

But I think the wider issue is that while law is often seen to respond to technology it is also reasonable to suggest that law reflects the society in which it is placed. At stake here then is whether Ambient Intelligence and other associated technologies really do represent a change, radical or gradual in how our societies operate and are structured, from the manner in which humans interact with one another, or even with how we as humans interact with machines.

I think it is reasonable to argue that current data protection regimes are not high on individual agendas for at least certain demographics in society. Examples here include the widening use of facebook, twitter and a raft of other 'social networking' sites, where while some people maintain strict control over their privacy others do not. Indeed recent news from the UK suggests that some 30% of divorces are now drawing on evidence gathered from facebook.

But is lack of individual concern and awareness of privacy really not present? At least in the UK context recent data losses have propelled concerns over privacy to be seen by people as an issue (use the example of the Information Commissioner in the UK). Likewise when an individual suffers a breach of their data, or an abuse of it, it would be expected that they would see and regard data protection regulations as a priority for themselves.

Is it then to be seen as an 'insurance' system of some kind? Only responsive when individuals exercise their right to privacy as opposed to proactively guaranteeing and supporting said right.

One issue that I think immediately creates a concern with ambient intelligence and data protection directives is the definition of and responsibilities associated between 'data controllers' and 'data subjects'.

While not succumbing to wild futurist visions, it's clear from even a superficial examination of how these environments are to be constructed and operate that the boundaries between data controllers and data subjects may become increasingly blurred. Is my PDA which is remotely storing data on you in order for it to make a decision for me to do something? How will data be traced in order to assign the status of data controller to someone or an organisation, especially if there is a level of end-user interactivity with data (for example imagine environment specific guestbooks as they appear on the web, except users may comment on particular services, provide hints and tips for other users, and so on).

One response to this has been to see Privacy enhancing technologies, whether as a form of system design or device, as a way of automating data protection. But this really suggests what has been termed the Design Turn in ethics, whereby we are just looking at technologies to solve problems.

We have to assume that in ambient intelligent scenarios what is occurring is the potential blurring of the lines between digital, virtual, online and offline. The network will be pervasive, real-time and physically modelled in environments that respond to us. Social connectivity will be paramount (but how much of this will be human-machine rather than human-human is open to debate).

If this is the case then really it can be argued that narrow conceptualisations of privacy as informational will not fully grasp what is going on. Perhaps we will return to spatial definitions, the idea of privacy as non-interference, (ie., do I really want your robot pestering me?).

This isn't to deny that data protection may continue to be important in some regards, but that Privacy will take on new dimensions (or even a return to 'old' conceptualisations) that are not sufficiently captured by the law at present. But I think this is also true for ethics and policy as well. At present we lack a regulatory and analytical vocabulary for means in which the issues can be dealt with or resolved [at least in policy and ethics]. Do we require an Ambient law as Hildrebrandt suggests?

The issue as far as I can see it is how do we reconcile various meanings of privacy, understanding as well that privacy (as the technologies themselves are) is grounded in societal structures. We can point to the fact that privacy has emerged as an issue in western contexts relatively recently. We can also point to the fact that privacy and how it is viewed varies from one society to the next, in sometimes greatly differing ways.

But there is the conflation then between data protection and privacy. I do not think that one equals the other. Privacy is certainly not set in stone, its elevation to a fundamental right, through Article 8 and the Lisbon treaty is laudable but does it have any resonance with citizens. I have tried to highlight that at least, if we consider ambient intelligence environments, I feel it will be unworkable (or heavily automated, which brings other issues into play).

But we as commentators then perhaps fall into the trap of caring when no-one else does. As Emile Aarts has suggested, Philips is in the business of selling products that users want, and importantly enjoy through positive experiences. If this is the case, and if we are to empirically examine trends, say amongst younger people, in the way in which they manage their identities, virtual or real, are we then in a position of being out of date and even out of touch.

If ambient intelligence is therefore a commercial success when these environments are realised, do we resort to being 'nannies', protecting people for their own good, etc., and my opinion is that this is just as problematic as automating data protection through technological means.

I think there is an urgent, clear and demonstrable need in that, as much as the 'expert' dialogue is open and ongoing, a reasoned engagement with the public is just as vital—on issues about the meanings of privacy, its value and worth, its relevance, and what wider groups of stakeholders envision as being the problematic or celebratory aspects of a world of ambient intelligence.

Without this engagement, and without a serious re thinking about the limits of privacy, and the limits of data protection, I think it is reasonable to conclude that data protection will be revealed as not being fit for purpose. A responsive modifying directive I think is also problematic, there will always be new technologies, new ways for users to interact with, use and experience them. I am not sure, as this remains a work in progress, what we can propose to replace it. In fact, and in summation, I would conclude that research must proceed in delivering answers that are empirically grounded, inclusive of stakeholder and public views to match ongoing expert driven discussions on these challenges, risks, issues and means by which they might be resolved.