The Future Internet: The Social Nature of Technical Choices

A SEMINAR ORGANIZED BY SESERV

Privacy Session

Key new technologies

eHealth	Central and distributed Electronic Patient Records (EPRs), National Programme for IT, Internet of Things, Microsoft Health, Google, chronic health management
Delay-Tolerant Networking (DTN/ICN)	Delayed/disrupted data, residual knowledge (ties in to most of the rest technology areas)
Social Networks	APIs, data flows, groups, digital tsunami
Search / Comparison	Vendor Relationship Management (VRM), Mydex, personalisation
Financial Interactions	Square, loyalty cards, ‘allmydata’

Challenges

1. **eHealth**

Security and privacy are often viewed as binary, not analogue issues. In addition, the existence of certain technologies does not mean that they actually become deployed in the environment where they are needed. Paper records are easier to lose but they also provide facility of access, subject to public scrutiny (medical records clerk supervising the process), as one of the participants noted. Regarding electronic records, the discussion focused on the challenges of appropriate access controls. When allowing online access to a large number of people, the reciprocity and transparency are lost. Connecting for Health was mentioned as an example of the problems arising when a large number of passwords is required. The group discussed whether there could be middle solutions allowing proportionate access, other than the existing laissez-faire or extremely regulated (access overformalisation) modes of professional access, even regarding unusual health conditions. The fragmentation of NHS communities who connect on health systems presents further challenges. Moreover, isolated instances or even hypothetical cases, instead of specific evidence, are often imputed to prove real harm and overtake any general benefits.

The government was identified both as a beneficiary *and* a stakeholder. It was suggested that it is always best when there is more health information, as long as the government does not know anything. However, there is still value in health information in terms of demographics and other government planning, but such information might also reduce government investment based on low incidence data. Government access to other kinds of data, such as queue data, was deemed viable, as long as these are not tracked back to the individuals.

Health data have both public and personal value. We would usually accept to sacrifice privacy for other benefits in a trust relationship. The responsibility for data lies with health professionals, who should represent the patients' interest in the system. Current approaches are taking away professionalism and might even lead to economic exploitation of data (digital taylorism), as it is attempted to unfairly put liability on people who cannot deal with it (over-delegation).

Issues with controlling correlation of health information include problems with the users of this correlation within the records, rather than with the correlation, which is useful in itself. The role of identity is also important here, as large anonymised databases might protect privacy, but we also need identifiers to develop useful correlations on emerging health issues.

Some people argued that from an IT perspective people do not focus on the use of systems in their context, but it was also mentioned that there is a lot of research on how consultations are taking place with the use of technology.

2. Delay-Tolerant Networking (DTN/ICN)

Challenges associated to Delay-Tolerant Networking (DTN/ICN) include issues of trust in relation to data mules, who might have an interest in the data being transferred, or might develop an interest in the future particularly if the data is not encrypted. Other problems relate to uses of data and to other users who might be able to access it, especially as DTNs are used in close-knit communities (the example of American soldiers in Iraq voting anonymously in the last presidential election when all their votes were faxed to their base was mentioned). If, for example, someone does a search for divorce or specific health information, privacy is compromised if this information comes back quickly (through village routers and proxies collecting these requests), because it means that someone else has accessed it as well. In this sense privacy becomes time-sensitive, since some information might be considered more sensitive over time or relate to something one doesn't mind disclosing but only later (e.g. after the divorce is filed or any health problems develop further).

In terms of storing and propagating data, the group discussed epidemic propagation and public peer-to-peer propagation. Filtering and categorisation of information and information-centric networks were also identified as challenges, but there was some doubt as to whether it would always be best to know what the information transferred is about. Knowledge in-transit is delayed in its impact and not controlled in the same way (in-transit v at-rest). Other parameters considered important include privacy by design and trust-based routing, in the sense of generating trust by requesting something to be delayed or indicating it as sensitive. The discussion also evolved around legal boundaries and cultural differences in what different communities find appropriate to expose.

3. Social Networks

The group agreed that privacy and security are usually built in later in social networks and discussed where the responsibility for that might lie. Social networks usually have to catch up with the expectations of their users about the boundaries between public and private spheres, but that might not always mean that evolution is user-based. Self-organisation and structure are important elements of social networks that should be taken carefully into account. The participants compared social networks to their group, where, unlike social networks, connection is equivalent as they know who was there and who heard what. On Facebook, for example, there are latent connections. Social networks might create vulnerabilities and liabilities, in terms of people one is linked to who they might not know. If we are more active in organising our links, we self-organise and produce structure in our social network. Expiration dates were also noted as relevant. Social networks would encourage you to do things that make it valuable. But there are differences in how people prefer to manage this structure, as, for example, students *want* to keep latent links. This puts emphasis on privacy as contextual integrity. The participants also compared social networks to small offline communities where one knows the people forever, in contrast to the dispersed network links online.

It was further argued that social applications take away the real social interaction and that the users' understanding of privacy implications is limited. The ability to see who looks at your data and realise the privacy implications, or an increase in commercial activity, might change user behaviour and privacy management. However, it was also argued that social networks sometimes function as an index for building actual, real social networks (the example of freshers in a US university was mentioned) and that there are competing networks with more privacy control which do not attract so much attention.

Sources of expertise

1. eHealth

There is a culture gulf between practitioners and IT supply, with islands of people producing materials in different language. The following differences were noted:

Practitioners	IT people
Bottom up, practice driven innovation	Principle approach
Dependability	Not well geared to health interests
Different uses of system capabilities	Delphi v focus groups

Other sources of expertise include directives, legal texts and legal academics.

2. Delay-Tolerant Networking (DTN/ICN)

As this is a novel technology there are few resources of expertise, apart from the Internet Research Taskforce (IRTF) DTN specific group. Technologists draw requirements from user expectations and behavior and therefore it is useful to talk to people who are used to dealing with time delay (e.g. Laplanders).

3. Social Networks

Counter-movements such as Mydex, diaspora, Internet of Subjects, as well as popular media are used as sources of information.

Strategies

Firstly, participants noted the importance of different groups acknowledging each other's expertise (for example health practitioners and IT). There was discussion on whether it is best not to try to design a system but to allow it to evolve in ways that involve the people within it, especially with regard to health care. Multi-perspective principles were identified as another important strategy, together with Tussle analysis, which would provide feedback to legislation. Further, participants debated the value of constraining user innovation to achieve lock-in and thereby protecting privacy. Privacy principles are persuasive and propagate through the environment, influencing people's behaviour. Natural experiments were also mentioned as another useful strategy. Closing the session, the group contemplated whether more openness and connectivity are always better and whether social networks are essentially self-referential.