A roadmap for interdisciplinary research on the Internet of Things: Social sciences

5 January 2013

Lead author: Professor William Dutton
Oxford Internet Institute, University of Oxford

With: Licia Capra, Marina Ciaraldi, David F. Evans, Anthony Furness, Ian Graham, Marina Jirotka, Agnes Kupai, Martin Maguire, Nigel Matthews, Miranda Mowbray, Malcolm Payne, Alison Prendiville, Ed Steinmueller and Rachel Tyrrell

Contributors: Dr Licia Capra, UCL; Marina Ciaraldi, Sheffield; Dr David F. Evans, Derby; Professor Anthony Furness, University of Sheffield; Ian Graham, Edinburgh; Marina Jirotka, Oxford e-Research Centre, University of Oxford; Agnes Kupai, BASF Medals Recycling; Martin Maguire, Loughborough University; Nigel Matthews, PFI Knowledge Solutions; Miranda Mowbray, HP Labs; Malcolm Payne, Trusted Renewables; Alison Prendiville, C4D, University of the Arts, London; Ed Steinmueller, University of Sussex SPRU; Rachel Tyrrell, Principal Policy Manager & Deputy Team Head, Health & Human Behaviour, ESRC

Contents

1 Introduction

The UK's Technology Strategy Board (TSB) has supported a Special Internet Group (SIG) focused on the Internet of Things (IoT). This is one theme that emerged from discussions within the Future Internet Systems Group (FISG), also supported by the TSB. The UK's Research Councils (RCUK) are interested in developments around the IoT, given the potential of such innovations to engage all the disciplines, and its potential centrality to RCUK digital economy programmes and a proposed Connected Digital Economy Catapult (CDEc) that would be supported by TSB. This report is a summary of discussion within one breakout group of a roadmapping workshop organised in collaboration with the RCUK, that focused on developing a multidisciplinary understanding of the IoT and the kinds of research that should be supported by the respective research councils.

The roadmapping workshop was aimed at informing the development of research and development programmes as well as commercially oriented initiatives of the IoT SIG and the CDEc. This particular breakout group focused on social and ethical aspects of the IoT, identifying research that would be of value to understanding the social, legal and ethical factors shaping the IoT and its implications for individuals, organisations and society at large in the UK.

A major risk in a focus on the IoT is that it will prioritise a focus on the technical artefacts and ignore the social aspects of the large technical systems or information infrastructures that they will require. Many of the technical issues of standards and design are challenging, and there will be a strong push for technically focused research and development. And as discussed below, it will be hard to draw social researchers into this relatively new area of technical innovation. However, social scientific research perspectives will be critical to challenging many of the common, taken-for-granted assumptions about the IoT. Moreover, some of the social and economic implications – intended and unintended – are potentially killer issues, such as issues around privacy, that could undermine efforts to exploit these developments.

For such reasons, the Economic and Social Research Council (ESRC) needs to play a significant role in study of the IoT. It cannot look to computer scientists and engineers to set the agenda for ESRC research, despite the hard technical aspects of this area. Social scientists should be scoping the social and economic issues that will shape the design, development and implications of the IoT, and developing a strong research agenda around these issues – all of which should advance theory and research on society and the internet more generally.

1.1 The multidisciplinary nature of the Internet of Things

The formation of a SIG on the IoT arose around a belief in the need for multidisciplinary research on this topic.[1] The immediate focus was the design of a workshop, which resulted in this roadmapping event, held in Loughborough in July 2012. This start was judged to be

[1] A multidisciplinary team was put together around Professor Rahim Tafazolli, CCSR Director at the University of Surrey. Rahim was a member of the FISG and is an engineer, focused on mobile communication systems. However, representatives of all the Research Councils are included in the SIG and charged with advising the SIG.

important in defining a clear set of issues for multidisciplinary research that could be identified before the SIG moved forward. The aim of this White Paper is to record and further the SIG's commitment to consider the wide range of ethical, social and economic issues in charting directions for research on the IoT, which was the focus of the breakout group, whose discussions are summarised here. As a breakout group over two half-days, the summary is not designed to be comprehensive, but seeks to be indicative of issues that this group considered critical to a research agenda that encompassed the social, legal and ethical dimensions of the IoT.

1.2 Keeping definitional issues open

There are definitional issues over what the IoT encompasses. The workshop summary notes that:

> 'The Internet of Things (IoT) is one of the terms widely used for the set of technologies, systems and methodologies that underpins the emerging new wave of internet-enabled applications based on physical objects and the environment seamlessly integrating into the information network.'[2]

In many respects, the IoT captures the next stage of the internet's development, moving from connecting people to one another and to documents and data to connecting devices that can operate in systems with the aid of intelligent agents, and people. Arguably, this is not new.[3] Even early demonstrations of the internet sometimes focused on links with things, like a coffee pot. However, the scale of developments around connecting things is growing in scale, sophistication and application. For example, since the workshop was held, the IoT has become one market-led programme of the UK's Satellite Applications Catapult.[4]

Given the pace of change, it is important to leave the definition of the IoT relatively open. First, the IoT is evolving rapidly, and the boundaries between the IoT and the internet of everything else is permeable and blurred. People are clearly an aspect of any IoT, such as in smart metering, where people design these technologies and are expected to read output in the household, the utility company and wherever data is shared. Definitions can shape theoretical perspectives. For instance, an overly narrow technical definition of the IoT could undermine a social research agenda.

1.3 Differentiating the Internet of Things from the internet

Many discussions about the IoT fade into discussions of the internet generally, as the distinctions are often difficult to maintain. Privacy and data protection issues, for example, revolve around the IoT but are quite similar to evolving discussions over privacy around the internet more generally. Similarly aspects, of issues around the IoT are involved with some technologies in use with the mobile Internet, such as GPS and near field communication

---

2 TSB (2013) *A roadmap for interdisciplinary research on the Internet of Things*, London: Technology Strategy Board, p. 4.

3 An IBM video has provided a cartoon-like but accessible overview of the basic idea; see: http://www.youtube.com/watch?v=sfEbMV295Kk

4 https://catapult.innovateuk.org/satellite-applications

(NFC).[5] That said, as discussed below, the IoT brings new opportunities and threats to privacy and data protection and is therefore critical to highlight within any IoT research agenda.

1.3.1 People as objects

Some participants reminded others that people are objects, and the body is an object, making people part of the IoT. For example, web cameras combined with face recognition technologies make the person one more object. In such respects, will it be possible and desirable to make a clear distinction between the internet and the IoT? Will people even know they are part of the IoT? They might not. In many contexts, the IoT will be invisible to people, who are unlikely to realise the depths and frequency of their interactions with IoT systems. This 'unconscious exposure' teases out issues of consent and trust that might be more central to the IoT than to many other internet applications that are more consciously used by people.

1.3.2 Data sharing

However, the IoT carries with it an inherent assumption that information will need to be shared across things, applications and possibly sectors in order to be most useful, such as in using energy or water meter readings to alert a family about the health of an elderly parent living alone. This data-sharing assumption might lead to the IoT having even more dramatic impacts on privacy and data protection than other information and communication technologies (ICTs).

1.3.3 Scale matters

There are fewer than ten billion people on the planet, but one organisation – HP – foresees there being a trillion sensor devices.[6] Data storage needs to cope with this expansion inherent in the IoT are huge as well, even if storage capacity is doubling every 18 months. The scale of the IoT could simply dwarf that of the internet of today. The potential scale of its societal implications is equally enormous. However, there appears to be a lack of appreciation, by researchers, the public, policy-makers and industry, of the social implications of this scale and the pervasiveness of its application across all sectors of society.

1.4 Contexts and applications are key

Likewise, it is difficult to speak clearly about the social aspects of the IoT, such as underlying business models, without focusing on particular areas, ranging from monitoring medical conditions to turning on household appliances to environmental sensors. Surveys and case studies of the use of the IoT in various social and institutional contexts will be critical to grounding discussion of the IoT in concrete empirical realities. Nevertheless, much discussion of the IoT is often conducted at a high level of abstraction, as the IoT generally, or in a universal and ill-defined context. It seems difficult to speak in any detail about the social

[5] http://en.wikipedia.org/wiki/Near_field_communication

[6] http://www.hp.com/hpinfo/newsroom/press/2009/091105xa.html

uses and implications of such innovations without focusing on specific contexts of use. As cases in point, consider the different social implications of the IoT for an ambient kitchen, performance art (such as dancers wired with sensors), health monitoring, home energy meter reading, monitoring pollution in a river, traffic flows, and so on. Systems have very different applications and contexts, which make discussions of their societal implications more meaningful when anchored in specific applications within a particular context.

1.5 The centrality of the social sciences

The social sciences should be very central to research on the IoT. The IoT is tied to many research areas already in place, such as work on the social implications of the internet, privacy and data protection, digital research and digital social research, including new issues of big data, and data analytics, and implications for services and the quality and value of information to the general public and other users. Much can be drawn from related research areas, such as digital research, to jump-start more social research on the IoT.[7]

The following sections of this report indicate key ways in which the social sciences can be brought into the study of the IoT, such as by looking at the IoT in context, describing and critically exploring the infrastructures of provision, focusing on the tensions involved in key policy choices, prioritising the social dynamics of innovation, further scoping of the social, legal and ethical issues at stake, taking account of the social shaping of the technology and examining key issues of governance, policy and regulation applicable to the IoT.

2 Empirical studies of the IoT across multiple contexts

Issues of trust, norms, open versus proprietary data, and more are likely to vary substantially across different contexts of use and application. However, it is difficult to predict these differences unless there is a careful body of empirical work on how users view these technologies in different contexts, the choices they make, and the implications they have in actual settings of use. Home energy meter reading will be different from remote monitoring of health and related medical conditions. Sensor networks in the desert to monitor seismic activity and their effects on motorway bridges will be quite different from monitoring pedestrians in public places or having a ‘smart wardrobe’.

2.1 Towards a typology of social, legal and ethical contexts of the IoT

There would be value in the development of a typology of the IoT from a ‘context of use’ perspective, such as reflecting the physical environment in which it is embedded, ranging from large scale buildings, to personal items – biometric passports and health self-monitoring devices. Categorisation of these contexts of use could help illuminate and concretise our understanding of the IoT.

There may be aspects of the IoT that are quite generic, but many will be influenced dramatically by the contexts within which it is developed and applied. Different social, legal

[7] See for example, Dutton, W. H. and Jeffreys, P. (eds.) (2010) *World wide research: Reshaping the sciences and humanities*, Cambridge, MA: The MIT Press.

and ethical issues will be faced in these different contexts of use. A few examples from different arenas of activities help illustrate the significance of context:

- *Creative digital economy*. Will the IoT be the new thing for creative digital businesses and applications? In a time of austerity and governmental cuts, will the IoT be a solution or a frill that will need to await a time of more slack resources? Alternatively, will applications tied to the IoT be perceived as a low-cost way of providing services, harvesting information, inspiring new creations? Will social, legal and ethical issues be perceived as stifling creative innovation in business and commerce, and thereby be at risk of compromise?
- *Smart augmented cities*. Cities and communities often arose as a context of use and application. One participant argued that the battle over open data was being fought for the 'heart and soul of smart cities'. Open standards would allow citizens and places to interact with one another. A presentation from Living PlanIT[8] spoke of creating 'The Urban Operating System' (UOS™) for industrialisation of the internet, viewing the city as a platform for the IoT. For example, augmented reality could be defined as part of an IoT. Who will control what links are made to quick response (QR) codes, or codes embedded in images of your house, your face? What will be appropriate or ethical, and how will such standards be developed and regulated, if at all?
- *Intelligent transport*. Global positioning systems (GPS) in cars and personal devices, such as mobile phones, have already brought the IoT squarely into the support of mobility and transportation systems. The workshop spoke of technologies ranging from motorists being guided into fields by GPS systems to whether military drones were part of the IoT.
- *Health and medical care*. Some of the crisp examples of the IoT cited in the workshop were tied to health and medical devices, ranging from mobile applications, such as a mobile application that enables users to monitor their own heart rate in real-time, to a medical team remotely monitoring individuals with serious medical conditions. Issues of privacy, ownership of data, and control over its use, arise around such innovations.
- *Law enforcement*. Devices are already used to monitor released prisoners, such as those on a home release curfew. Electronic monitoring is already a controversial issue, but new devices and systems will create an incentive for greater application, more precise tracking, and archiving, promising to raise the level and nature of debates surrounding this area of application.

3 Infrastructures of provision

Infrastructure studies are a rapidly growing area for science and technology studies.[9] In this area, social scientists describe technical infrastructures in ways that explain how small changes can have major social and policy implications.[10]

---

[8] http://living-planit.com/

[9] Edwards, P. N., Jackson, S. L., Bowker, G. C. and Knobel, C. P. (2007),'Understanding Infrastructure: dynamics, tensions, and design', Report of a Workshop on 'History and theory of infrastructure', Ann Arbor, Michigan, January.

[10] Sandvig, C. (2013), 'The internet as infrastructure' in Dutton, W. H. (ed.) *The Oxford Handbook of Internet Studies*, Oxford: Oxford University Press, pp. 86-108.

3.1 Centralised versus decentralised infrastructures

Social and legal issues are likely to be shaped by the ways in which services are provided, such as via cloud computing or more decentralised storage and retrieval at the end of the pipe. Research needs to focus on embedding this full range of arrangements for provision to examine such issues as whether privacy and data protection are exacerbated in some IoT infrastructures, such as in the cloud. Where is data collected, analysed and archived, by whom and under whose control? With whom is it shared and under what provisions?

3.2 Reviews and experiments with alternative user-interface designs

Other infrastructure issues arise around human–computer interface designs. Some sets of issues might be amenable to experiments, such as with alternative user-interface designs or technologies. For example, should social, legal and ethical designs be hard-wired into the IoT, or should users be able to choose and control settings? Will choice leave some groups or individuals more vulnerable, such as those with lower levels of digital media literacy? Will societal divides be widened or deepened, such as around age and poverty, by choices that are less controllable by those who are older or less well to do? There are already designs based on users moving their fingers or making other physical movements, such as hand waving.[11] Will these designs open up the IoT to new users? What problems will be posed by 'refusenicks' who decline to use or employ particular applications of the IoT? Will non-use be possible or feasible in a connected digital economy?

4 Focus on tensions in information policy choices

Within any context, the group felt that it would be productive for developing a research agenda if there is a focus on key tensions or controversies that might be addressed by social science research. Some the tensions identified by the group are outlined in Table 1. While this table admittedly oversimplifies policy choices, it does highlight the diverse ways in which an IoT could be developed, such as in open or proprietary systems (Table 1).

[11] An example is Leap Motion: https://leapmotion.com/

Table 1 Focal points of policy tensions around the IoT

Tensions	Low control	High control
Access	Open	Proprietary
Innovation	Freedom and incentives to tinker	Quality control
Standards setting	Agreeing a small set of standards to enable interoperability	Enabling diversity but risking fragmentation across a proliferating number of standards that might threaten interoperability
Governance	Create incentives, such as for transparency	Mandate policies, such as over transparency, and readable terms and conditions applied to data
Social science approaches	New digital social research	Traditional methods, brakes on digital research
Choice	Enable people to decide what they want devices to do, provide others, etc.	Limit choice to enable more predictable systems that meet expectations
Data integrity	Lots of copies to keep stuff safe (LOCKSS), archived	Few copies to control access, accuracy and guard privacy
Data retention	Open to providers, users	Minimum or maximum standards required
Forgetting	Individual choice, education, digital literacy	Regulation on right to keep or forget, change information
Identity	Multiple and evolving	Single and persistent

5 Prioritising the social dynamics of innovation

A central issue for the SIG and the TSB's CDEc will be how innovations around the IoT can be fostered in the UK as a means to support economic development. Of course, the dynamics of technological innovation have been central to decades of social research, and the social sciences should be key to addressing such issues. Major technological innovation in the workplace, household or other social settings often requires changes in how we do things – social and cultural innovation, not simply technical change. For example, the productivity benefits of many ICT innovations in the workplace are not realised without re-engineering the way work is done. It is therefore important to track innovations around the IoT, and the factors that facilitate and constrain the social innovations, ranging from incentive structures to business models underpinning their adoption.

Beyond technical innovation, adoption of the IoT is likely to require major organisational and service innovations as the IoT will require new partnerships between organisations (e.g. insurance companies and in-car navigation software providers to tailor insurance policies to individual driver behaviour). Identifying such partnerships and the successful business models behind them will be invaluable for understanding innovation within this area. Do organisational IT departments have the right skills and paradigms in place to exploit the IoT?

The scale and reach of companies involved in the IoT is likely to be polarised. On the one hand, companies such as Philips and Electrolux are involved in large-scale global projects,

while SMEs such as BERG London and Cosm (previously Pachube) are more likely to be locally focused. What are the different innovation strategies used in such diverse business contexts? Are there knowledge transfer lessons that can be shared between business-to-business and business-to-consumer contexts and small-to-medium- to large-scale organisations?

Despite the problematic notion that the IoT does not involve humans, people will be directly involved in adopting and sometimes paying for systems. If households do not look at data from their energy meter after the initial novelty wears off, if at all, then much of its expected utility will be lost. It is not wise to assume that there will be a market for the IoT in many social contexts with respect to many applications. At the same time, it is unrealistic to expect the public to know in advance if they will value such innovations. Uptake is tied to a variety of social and economic factors that will shape access to, take-up and use of the IoT, such as geography (rural versus urban), economic resources, age and life stage, and more.

Of course, innovation is just one of many issues relevant to the social, legal and ethical issues of an IoT.

6 Scoping studies of the social, legal and ethical issues

The workshop helped to jump-start an effort to scope the range of key social, legal and ethical issues tied to the IoT, such as around data (ownership, rights, retention, forgetting, control, access, rights, such as rights to machine-generated data), networks and other aspects of the infrastructure of the IoT (see Table 2). More systematic efforts to more comprehensively survey, identify, classify and further scope the wide range of issues would be of value to research in this emerging area.

Table 2: Social, legal and ethical issues of the IoT

Issue	Description	IoT example(s)
Privacy and data protection	Ensure against unauthorised disclosure of personal information	Personal information is everywhere in the IoT—how do we even find it?
Privacy as peace of mind	Avoid invasion of personal space and expectations	Intrusive surveillance in a private space
Choice	Should users be offered choice in the use of the IoT? Will the IoT increase or decrease choice?	Energy monitoring might need to control use of household appliances, overriding user preferences
Social issues of devices associated with individuals	A mobile phone can be used to track one's location, for better or worse	Widespread comfort with a mobile phone; what about apparel?
Security	System and data kept secure from unauthorised access, such as by hackers	Remote monitoring of devices, spaces, data
Ownership and intellectual property rights	Clarity over who owns what data, right to use data, …	Who owns data about your physical condition, e.g. heart rate, walking speed
Control	Clarity over who controls use of data or systems	Energy solutions may take control away from individual households
Safety and protection of the public	Sensor networks on bridges and roads can monitor seismic activity, providing early warning of risks	Public webcams can be used to improve the safety of particular areas, or will they displace crime?

Table 2: Social, legal and ethical issues of the IoT (cont.)

Ceasing of action, and planning for obsolescence	Who can stop a system; and who is responsible for the implications of ceasing?	What happens to a person's things and the data about them when they die?
Geography of benefits and costs	Will the benefits of the IoT be concentrated in affluent nations and costs, such as waste, concentrated in the least affluent?	Developing nations are now bearing the brunt of electronic waste
Biodegradable	Will trillions of things pollute the environment with more electronic waste or be designed to biodegrade?	Mobile phones are essentially not biodegradable, and are toxic
Energy consumption of the constantly connected	Server farms consume large amounts of energy to support cloud computing, with a disconnection between usage and environmental cost	Is the rise of the IoT likely to increase the need for greater energy consumption, or reduce carbon emissions, such as by smart transportation?
Data retention	Forgetting, retaining, archiving, curating data generated by the IoT	Will people be able to stop the ability of others to track their whereabouts through the things they wear, such as their phone?
Ethical aspects of designs	Can privacy be designed into the IoT? Are there links to developments around responsible innovation?	Will privacy designs undermine the viability of some applications, such as location-based services?
Cultural practices	Do systems align with the cultural practices of different groups? Do they presuppose a particular cultural context?	Will services be available in multiple languages?
Educational policy, teaching and learning practices[12]	Can the IoT support learning through making, physical construction with coding and hacking technology?	Will new learning tools develop, such as programming electronic blocks?[13] Will the IoT place a burden on the educational system, requiring students to be taught an IoT literacy?
User engagement in design, such as living labs	Can researchers become involved in participatory design where users are actively involved in the co-designing of IoT services, especially in information interfaces and creating seamless services?	Field research on the actual use of the IoT in different contexts of use.
Implications for value of property, buildings, etc.	Will the IoT become a standard feature of automobiles, cities and workplaces?	Will a smart home or building be more marketable?

A few issues stood out as most significant in shaping the viability of the IoT.

[12] NESTA recently produced a report in this area: http://www.nesta.org.uk/areas_of_work/public_services_lab/digital_education/assets/features/decoding_learning_report

[13] See http://itee.uq.edu.au/~peta/_ElectronicBlocks.htm

6.1 Privacy and data protection

There was much discussion about how people feel about 'giving away' their information, or enabling others to harvest information based on their behaviour. Some people seem very cautious about giving away details, such as by using social networking tool facilities to set boundaries around who can see the different levels of detail. Others are more relaxed or blasé and more inclined to give away any information about themselves for very small rewards. This division might be generational, with young people, as some argued, being most vulnerable to exploitation, but others argued that the young have higher expectations, increasingly feeling that they have and should have the ability to control who knows what about them, compared to older people. However, if something goes wrong and say a person's details get displayed inappropriately somewhere this may change that individual's attitude to keeping personal data more private. There is the possibility to carry out research into the public's attitudes to privacy in relation to online systems that could lead to recommendations for what is good practice for handling such data. Research is also likely to point to the need for awareness raising among the public at large about what is actually done with their data, how it may be used and what they can do if they wish to take control of it in some way.

6.2 Global misinformation systems

We had a lively discussion of the tendency of people to collect more information than they can use. All the various actors involved with the IoT are likely to err on the side of getting and harvesting more information than they need. This was a classic issue with management information systems in the earliest decades of data processing, and the internet and the IoT is bringing this problem of what Russell Ackoff called management misinformation systems to the general public at a level that Ackoff could not have anticipated.[14] The enthusiasm and hype surrounding 'big data' is likely to exacerbate this data deluge, as data becomes perceived as new resource.

6.3 Big data problems

In a growing variety of contexts, the IoT will be generating huge quantities of data that can be imaginatively applied as indicators of social behaviour. The analytical value of this data depends on the exact traits that are captured, the population from which it is harvested, and its availability, such as whether it is locked up in a proprietary context. Large quantities of data are not necessarily valuable and can be misused in ways that lead to invalid inferences. However, the data generated by the IoT in the course of everyday life and work will undoubtedly generate data at levels that will present greater opportunities and risks, such as with respect to ethical guidelines. The design and visualisation of data will affect levels of engagement and risk; it will also have the potential to enhance transparency in data sharing and reduce other negative aspects of the IoT, if data visualisations are designed in relation to users' interests.

[14] Ackoff, R. L. (1967),'Management Misinformation Systems', *Management Science*, 14(4): B147–B156.

6.4 Public attitudes, opinions and behaviour

There was much discussion of the degree to which the public care about privacy, data protection, and other social issues of the IoT, as opposed to the benefits the public might expect in public safety, energy conservation and lower costs. Some research has found that the public's concern over privacy related to ICTs, such as the internet, remains substantial,[15] but many are still willing to give it up for safety or convenience. It has been characterised as a mile wide but an inch deep,[16] but that does not mean law and policy should not protect privacy.

6.5 Tightly coupled systems

Societal implications might be tied to the IoT leading to the development of increasingly large scale, highly coupled technological systems that can remove human intervention to be more reliable but also increase the potential for societal vulnerability, as with major system crashes.[17] Loosely coupled systems might be more flexible and more capable of adapting to unexpected changes. In this respect, will the development of an IoT create more serious societal risks?

6.6 Quality of service issues

The view that the IoT will lead inevitably to a higher quality in the provision of many services is problematic. The use of automatic voice commands in automobiles was quickly rejected. Most drivers viewed them as a distracting annoyance. Smart homes with motion-activated lights often create havoc with lights being activated by pets or people at the wrong time, or people running around in a room in order to switch the lights on. Many of these failures might be put down to early design flaws, but they point out the challenges of ensuring that any technological logic addresses more central concerns over the ends tied to the IoT as a means, and not an end in itself.

6.7 New forms of risk: your refrigerator is calling

Beyond privacy and data protection, does the IoT open up new forms of societal risk, or exacerbate existing issues of risk? Will there be new threats to identity theft, for example? Will misunderstanding the purpose, intent or extent of a thing's function be inherently more dangerous? For instance, a new risk might revolve around the control of actuators. The IoT in general includes actuators as well as sensors. (Actuators are the devices that control a mechanism, such as telling it to turn on a light or send a message.) Actuators that are embedded in a public environment or that can act at a distance may affect people other than their owners. One possible new form of risk is that people who are adversely affected by such actuators (for example, being repeatedly telephoned by a public lavatory that has

---

[15] Dutton, W. H. and Blank, G. (2011) *Next Generation Users: The Oxford Internet Survey 2011*, Oxford: Oxford Internet Institute, University of Oxford.

[16] Dutton, W. H. and Meadow, R. G. (1987) 'A tolerance for surveillance: American public opinion concerning privacy and civil liberties' in Levitan, K. B. (ed.), *Government infostructures*, Westport, CT: Greenwood Press, pp. 147–170.

[17] Rochlin, G. I. (1997) *Trapped in the Net: The Unanticipated Consequences of Computerization*, Princeton University Press.

run out of supplies and has been programmed with the wrong number to contact the supplier,[18] or being locked in a building by its automated security system) may not find it simple to get the problem remedied. There may be malicious use of actuators, and adverse interactions between different actuators, as well as simple malfunctions and misprogramming.

6.8 Linking the IoT to work on responsible innovation

There would be value in linking research and development on the IoT to programmes developing around the concept of 'responsible research and innovation' (RRI).[19] The idea of an RRI programme would apply to all forms of innovation across business and research, and seek to influence policy and practice in both areas. RRI provides one example of a number of programmes that might embed consideration of the IoT and address some of the issues that surfaced in the workshop, but also move consideration of the IoT into other areas, such as such global issues as energy and climate change.[20]

7 Social shaping of the design of the IoT

More generally, can various visions of the societal implications of the IoT be critically assessed? There has been and will be much talk of the IoT improving travel, democracy, education and healthcare. While it is valuable to understand the potential of the IoT, it is also important to critically assess the feasibility of these scenarios and study the actual implications in context, such as noted above around infrastructure studies. However, there are myriad ways in which economic, legal, ethical and other social factors shape the design of technologies like the IoT, such as around user involvement and anticipatory design.

7.1 User involvement in design

Social research will be critical to the design of systems if they are to engage users. What devices look like, and where they are placed, can be major issues for users. Often it is impossible to predict these reactions without trials and study of actual users and the usability of different devices. Given the scale of resources being devoted to usability studies across the computing and internet industries, it will be challenging to find ways in which social science support will enable major insights on these issues, but it is also the case that industry can become trapped in particular models of provision that could be jettisoned by social research that has not invested in prevailing models. With the introduction of self-

---

[18] This actually happened in 1997: http://catless.ncl.ac.uk/Risks/19.33.html#subj1

[19] See Von Schomberg, R. (ed.) (2011) *Towards responsible research and innovation in the information and communication technologies and security technologies fields*, Luxembourg: Publication Office of the European Union. Retrieved from http://ec.europa.eu/research/science-society/document_library/pdf_06/mep-rapport-2011_en.pdf; Stahl, B. C. (2011) 'IT for a better future: how to integrate ethics, politics and innovation', *Journal of Information, Communication and Ethics in Society* (9:3), Special Issue on Emerging Technology and Ethics, edited by Kutoma Wakunuma, pp. 140–156; and Owen, R. and Goldberg, N. (2010) 'Responsible innovation: a pilot study with the UK Engineering and Physical Sciences Research Council', *Risk Analysis: An International Journal*, 30(11), pp. 1699–1707, available online at: doi:10.1111/j.1539-6924.2010.01517.x

[20] Links to relevant programmes include: Ethical Issues of Emerging ICT Applications (ETICA) www.etica-project.eu; and Framework for Responsible Research and Innovation in ICT http://responsible-innovation.org.uk/frriict/

monitoring devices in patient healthcare, for example, institutions such as the NHS will need to respond organisationally in order to deliver different types of services; patient–doctor relationships will also have to adapt. Interdisciplinary participatory design methods to co-design services can assist these changes but it requires an integrated approach between different stakeholders rather than a bolt-on approach.

Likewise, social research can often place more emphasis on designing for diversity, when industry might focus on early adopters. Given digital divides, by age and income, for example, there are likely to be radically different attitudes and values concerning the need for and desirability of an IoT, such as in the household, or in public spaces.

7.2 Designs anticipating ethical and legal constraints and requirements

Some applications of the IoT are likely to generate very sensitive personal information, making issues of privacy and data protection, ownership and security even more important. A simple example is an energy meter reading, which can reveal aspects of a household's routine behaviour that could be sensitive. This is illustrated by talk of its potential to provide services for seniors, such as calling a family member if a senior citizen does not get up in the morning. Some of the associated issues are transparency and consent. Will users, such as households, understand what is collected, by whom and for what purposes? Will they know if data is sold to, or used, by third parties?

Are there ethical issues tied to the IoT that are not simply related to ICTs in general? For example, will there be developing norms about the use of the IoT, similar to evolving norms about the use of social media? What could be the effect on norms of the IoT, such as by identifying people in a room? Will guidelines need to be imposed on providers of IoT, such as 'do no harm'? Some of the common ethical design issues are presented in Table 3.

Table 3 Ethical design of the IoT

Area	Description
Privacy by design	Privacy impact assessments, but also simply making privacy a priority from early stages of design
Security by design	Building security into systems from the beginning rather than downstream, once a technology diffuses
Value sensitive design	Building systems focused on particular values, such as moving control closer to the user
Impact assessment	Looking at the full range of social and economic implications, intended and unintended

7.3 Issues of governance, policy and regulation

Regulatory processes designed to cope with hundreds or thousands of transactions or services providers might need to be reconsidered in order to cope with a trillion things and the data they produce. Undoubtedly, new developments around the IoT will move faster than the law and policy, creating an almost certain crisis of governance and policy in this area.

These issues move quickly into issues of governance, policy and regulation, from consumer issues to industrial policy and economic development. Anthony Furness argues that many of the social and ethical issues of the IoT can indeed be defined as governance issues.[21] He has worked on a framework for discussing governance issues, based on his research in CASAGRAS (Coordination and Support Action for Global RFID-related Activities and Standardisation). Clearly, there is a need for study of appropriate models of governance for an IoT that can cope with the scale and pace of change in this area. Some of the key issues of governance and regulation include the following.

7.3.1 Aligning local, national regional, and global practices and policies

The workshop discussed the need to align our policy agenda with developments in policy and governance at local and global levels, such as across the EU. All of the issues besetting internet governance, ranging from jurisdictional turf wars to the institutional arrangements of governance structures will be relevant to the IoT.

7.3.2 Accountability and liability

Will the IoT increase or undermine and obscure accountability for failures, data breaches, costs, etc.? Who is responsible for failures, ranging from travel delays to life-threatening misinformation?

7.3.3 The politics of standards

Standards are widely viewed as critical, but opinions differ over the preferred standards. Those who set what standards will have major implications for the winners and losers in business and industry as well as national technology-led industrial policies.

7.3.4 Rethinking data protection

As discussed above, there was a general perception that the data protection act has not worked well in the present digital environment, and is not up to the task in the era of the IoT, which will operate at an entirely new scale of activity. What policy and institutional changes can be developed to cope with the IoT?

7.3.5 Control of devices

The development of devices such as digital companions, which will know and learn a great deal about their users, need to be governed by rules, or allowed to reveal and disclose anything about their user. An ‘anything goes’ strategy might be appropriate in early experimental phases but be inappropriate as the devices become more ubiquitous and capable of increasingly sophisticated communication.

Control of actuators may be just as sensitive as the question of control of sensors. There is a tension between the goals of security and quality control – which suggests limiting as much as possible people’s ability to interfere with the operation of an actuator – and the goals of

[21] Furness, A., ‘International framework for IoT structure and governance’, a paper for CASAGRAS2, an EU Framework 7 Project, and ‘The need for risk assessment and design methodology for supporting privacy and associated security in RFID systems’, CASAGRAS Discussion Document.

human autonomy and user-responsive technology, which suggest the opposite. For example, smart city actuators could become a mechanism for citizen empowerment, for infrastructure attacks, or for citizen disempowerment.

The IoT is likely to shift the boundaries between consumers and producers in, for example, local government services. GPS software is increasingly used as a way of involving local people in the up-keep of their environment and making them 'active citizens' (RFID bin tagging, smart phone GPS apps) or 'prosumers'. As local government services are scaled back, GPS in the IoT has the potential to open up a world of surveillance of citizens, representing 'surveillance as social sorting, as a means of management, influence and governance'.[22]

Exploring these issues of governance and regulation will require sophisticated and detailed understanding of the full range of actors involved in the IoT. Discussions often evoke overly simplistic models of the ecology of actors involved with the design, implementation and use of the IoT, such as focusing on users and providers, when the ecology is far more complex. Research on the social shaping of the IoT needs to uncover this complex ecology of the IoT in order to understand how to effect change and enable appropriate governance and regulation.

8 Constructing this area to enable social and economic research

As noted in the introduction, the workshop viewed the IoT as inherently multidisciplinary, since any application will have not only quite technical issues for enabling systems to operate, but also economic, social, legal and ethical aspects to consider. A valid concern is that social research could get marginalised particularly at a point in time that early systems are being developed – early in the so-called hype cycle associated with emerging technologies. Social research could also get marginalised if viable projects are not implemented in real social contexts, where social research can be the most valuable.

For such reasons, the ESRC and other Research Councils need to involve strong social science input in the early discussion of how to conceptualise this area of research. There is a risk that early discussions about the IoT will be too loosely defined, and not consider specific use contexts. If even they are considered, the contexts about which information is available at these early stages may be quite different from the uses that will arise as the IoT becomes more widely adopted. Social scientists need to work with computer scientists and engineers to help frame studies of use contexts with the foresight necessary to make useful recommendations for IoT design and development in practice that are years downstream.

This raises a final issue around drawing in strong social researchers, given that this is an area that is seen to be highly technical and to not have immediate and obvious relevance to the social and economic sciences. It could be useful for RCUK to develop material that can help illuminate the IoT and recruit social researchers and economists to studies of these emerging technologies. Social and computer scientists and engineers need to help clarify the definition and nature of the IoT in ways that will stimulate social scientists to raise

[22] Lyon, D. (2006) *Why where you are matters: Mundane mobilities, transparent technologies and digital discriminations*, Routledge (p.221).

critical research questions and develop an appropriate research agenda. Internet studies is one of the most burgeoning fields in the social sciences, but it remains at the margins of mainstream disciplinary research.[23] This is likely to be the case for the IoT without a major push from the bottom up – the researchers themselves. It is critical that this area is targeted at the research community and not only the research councils.

8.1 Methodological tools and approaches

A key incentive for social and economic researchers to be involved in this new area stems from the potential for the IoT to provide new methodological tools and data.[24] The real-time monitoring of social life is increasingly possible, with all the opportunities and risk that this brings. New methodologies and analytical techniques may be needed to mine this potential, such as in capturing and reducing the large quantities of research data that the IoT could generate in ways that provide genuinely new insights. The IoT is a new means to support social science research, but also a new threat to privacy, informed consent and other ethical issues for research. In addition, participatory design tools for co-designing new interfaces and services will require greater interdisciplinary methods between designers and social scientists.

9 Summary

Many of the technical issues of standards and design of the IoT are challenging and will necessitate a focus on technical research and development. But it is important that social science perspectives are not overlooked in the process, because they play a vital role in identifying and challenging assumptions about the design, implementation and impacts of the IoT. In particular, some of the social and economic implications – intended and unintended – are potentially huge issues, such as around privacy, that could undermine efforts to exploit these developments. Examples of the tensions, and resulting diverse policy choices, have been provided in this White Paper, but it is clear that the IoT merits more systematic scoping of the social science research that could advance the understanding and development of the Internet of Things.

[23] Dutton, W. H. (2013) *The Oxford handbook of internet studies*, Oxford: Oxford University Press.

[24] Dutton, W. H. and Jeffreys, P. W. (2010) *World wide research: Reshaping the sciences and humanities*, Cambridge, Massachusetts: MIT Press.