The Societal Impact of the Internet of Things

A report of a workshop on the Internet of Things organized by BCS – The Chartered Institute for IT, on Thursday 14 February 2013. The Chairs were Jeremy Crump (BCS) and Ian Brown (Oxford Internet Institute, University of Oxford).

Introduction

BCS– The Chartered Institute for IT held two workshops about IoT in February 2013. This report is based on the seminar held on Thursday 14 February 2013 at BCS on the Societal Impact of the Internet of Things (IoT), involving input from industry, regulators and academics. This report draws on the position papers prepared for the forum, and the resulting discussion, to provide an introductory overview of the current use and likely future impact of the IoT, the inherent challenges and risks, and issues of governance. Position papers were prepared and presented by Daniel Boos (Swisscom (Schweiz) AG), William Dutton (Oxford Internet Institute, University of Oxford), Katherina Kinder (Lancaster University/Leibniz Institute, Cologne University), Gerd Kortuem (Open University), Simon Rice (Office of the Information Commissioner), Sarah Spiekermann (Chair of the Institute for Management Information Systems, Vienna University of Economics and Business). Sessions were chaired by Jeremy Crump (BCS) and Ian Brown (Oxford Internet Institute, University of Oxford). The forum was opened by Roger Marshall, President Elect of the BCS.

Societal Impact of the IoT

The Internet has (traditionally) been seen to be about connecting people and information. We are now dealing with a level of abstraction beyond that. However, unlike the Internet, which is a concrete technical infrastructure whose design and architecture are well documented, the IoT is still primarily a vision and only part reality—individual IoT technologies and systems exist, but there is currently no coherent global IoT. Whatever form it takes, the IoT will most likely be an extension of the Internet; distinctions between the IoT and the Internet are therefore often difficult to maintain, and they raise similar issues and challenges, for example, surrounding privacy and data protection. That said, the IoT introduces new challenges, carrying with it an inherent assumption that information will be shared across things, applications and possibly sectors. 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); such as when energy or water meter readings are used to alert a family about the health of an elderly relative living alone, or when people are tracked, making them part of the IoT. The IoT also brings with it a new scale of development. There are fewer than 10 billion people on the planet, but there could be a trillion sensor devices. Worryingly, there appears to be a lack of appreciation of this scale, and the pervasiveness of its potential application across all sectors of society. While current IoT applications are still very traditional, there is likely be more radical, emergent, unpredictable, and user-led innovation in the future; just as we have seen with the Internet.

Predictions of the impact of the IoT on society often overemphasize technology's role and assume a causality that is not necessarily present. There is consequently a risk that study of the IoT will prioritize the technical artefacts (things) and neglect the social aspects of its technical systems and information infrastructures. Not only is a technology the product of a specific time and place in history, but technological advancements also influence the society from which they emerge. By focusing on IoT technologies and their impact there is a danger of overlooking the fact that many developments don't originate merely in the technologies themselves. Rather, we need to also focus on the reasons why different actors push for—or accept—the introduction of these technologies. We need to ask: what changes in society have made these technologies important, and what role have the technologies played in establishing these changes? Social science perspectives will play a vital role in identifying and challenging assumptions about the design, implementation and impacts of the IoT in various social and institutional contexts, and be critical to grounding discussion in concrete empirical realities. This will be particularly important for those social and economic implications—intended and unintended—that are potentially killer issues, such as privacy. It may also help us tackle the daunting task of understanding something as vast as a 'change to society'. Indeed, there is huge potential for social science research, given the changes the IoT will bring about in business practices and innovation, privacy, governance and regulation, and our everyday life and work.

Given there are almost as many interpretations of the term 'Internet of Things' as there are experts and interested parties, and given the significance and pace of change, the seminar agreed that the definition should be left relatively open. At present it is more accurate to talk about a growing number of 'Intranets of Things' or 'Internets of Things' (plural), rather than a single IoT. Nor is it necessarily correct to assume that all these pockets of development will soon or easily come together to form a global IoT—these systems often have little in common besides the vague notion of 'connecting things'. The fuzziness surrounding the term and the diversity of existing systems should be taken into account when discussing the potential risks and societal impact of the IoT. In a similar vein, the many visions of the IoT as a seamless and unobtrusive technology should also be challenged, given the current reality of a messy and visible assemblage of technological artefacts, human actors, and organizational elements. Descriptions of future scenarios should take account of breakdowns, assemblages of old and new technologies, and the different viewpoints of the involved actors, and should be rooted in specific contexts of use.

Definitional issues aside, there are high expectations for the IoT's potential to profoundly change our lives—and not always necessarily for the better. As these embedded devices establish complex networks of human and non-human actors in our public and private spaces, they have the potential to create new relationships between people and computers. Some stated benefits of the IoT include higher business productivity, increased energy and transport efficiency, and greater control and auditing capacity in manufacturing and supply processes. However, these need to be balanced against very real risks to privacy, security and resilience, both known and unanticipated. Of course, when discussing issues surrounding collection and use of data we need to be sensitive to context—the data produced by a sensing device associated with a specific individual is very different to the environmental data produced by a buoy floating in the ocean, and must be handled differently.

There are likely to be unanticipated consequences of the IoT that result from the sheer volume of data produced by many different sources, and its increasing connectability and reusability. Plans by governments and utility companies to roll-out smart metering[1] may aim simply to improve energy consciousness and efficiency in supply and consumption; but it's not difficult to imagine a scenario where energy meter data—which after all provides a record of our movements and activities—could be used to provide evidence for when we come in at night, if we leave children in the home alone (e.g. in a custody battle) or if we were where we said we were. This is quite apart from concerns about the hackability of smart meters and grids, and therefore over the security of their data and functionality. Monitoring the activities of certain patients (e.g. those with Alzheimer's) or the elderly with home sensors or meters may be seen as intrusive on their private lives, but might also enable them to remain in their homes for longer, if remote monitoring (for example) of energy usage patterns could provide an indication that things were still 'normal'. A change in usage pattern could indicate a problem requiring intervention.

Despite rapid technological development in many areas—particularly in health and business—research on the social impact of the IoT is still quite sparse. Most work has focused on identification of potential business benefits, and apart from privacy, much less is known about the current and future impact of the IoT on society more generally, for example as we start to interact with the city-wide IoT systems of so-called 'smart cities'.[2] Furthermore, much discussion of the IoT is conducted at a high level of abstraction, or in very general and ill-defined contexts. However, we can't discuss the social aspects of the IoT without focusing on particular contexts of use, whether that be monitoring medical conditions, controlling household appliances, or environmental sensing. What might hold true for IoT systems and technologies in the retail sector won't necessarily be true for IoT systems in home automation—and what is true in terms of electricity generation and distribution will not necessarily be true in vehicles and public transport systems.

The impacts of this technology on society will be highly complex and likely unpredictable; however, some general points are that:

[1] A smart meter is usually an electrical meter that records consumption of electric energy in intervals of an hour or less and communicates that information back to the utility for monitoring and billing purposes. Smart meters enable two-way communication between the meter and the central system and, unlike home energy monitors, can gather data for remote reporting.

[2] The concept of the smart (or 'intelligent') city describes the growing importance of ICTs, but also of social and environmental capital (in addition to hard infrastructure), in supporting the competitiveness and sustainability of cities.

- Organizational and institutional innovation is key to the viability of the IoT, as it will change the ways we do things.

- Problems could result from generation of large quantities of data that are not necessarily valuable or needed, and that can be misused in ways that lead to invalid inferences; but data generated in the course of everyday life and work will also present great opportunities, for example in the design of more efficient transport systems.

- Public attitudes, opinions and behaviour will be critical if the public cares more about privacy, data protection, and other social issues of the IoT—as opposed to the potential benefits in terms of public safety, energy conservation, and lower costs.

- Privacy and data protection will be tied to how people feel about giving away, trading, or enabling others to harvest information based on their behaviour.

- The IoT could lead to increasingly large-scale, highly coupled technological systems that can remove human intervention in order to increase reliability, but that also increase the potential for societal vulnerability, as a result of hacking or major system crashes.

- Whether the IoT will lead inevitably to a higher quality in the provision of many services is problematic.

- There may be inequality in access to data of value to individuals and communities from the IoT, paralleling other digital divides across societies

The Internet of Things and the Economy

The increasing availability of high-quality data collected and transmitted in real-time through cheap, ubiquitous hardware and connections will undoubtedly lead to scientific, technical, and commercial innovation. Industry is currently investing a huge amount in IoT infrastructure, and the opportunities for business are massive in terms of improvements in productivity, and control of supply chains and distributed real-time processing. The IoT is a dynamic world, and the technology is likely to develop faster than the regulation—there is a real sense that industry is moving forward and 'working it out' as it goes. But how much do we know about the potential of these technologies to support business competitiveness and success? What is the expected economic benefit? And how will it change the workplace?

To understand the IoT's impact on business—as well as on the larger society—it is useful to focus on the capacity of IoT applications to:

1. **Informate**, for example, by gathering information through sensors, to

2. **Automate** and prescribe activities, for example by allocating a function to a system or by supervising the fulfilment of an activity, and to

3. **Transform** activities, for example by redesigning a business process.

As IoT applications become widely used we need to understand how they interact with organizations and people, and how their actions are variously enabled or constrained. Sensor-gathered data may enable informed decision-making by managers, but automated checks might also constrain a person's freedom to act differently. Of course, in real-world settings, people may use a technology differently than intended, may influence its capacities by changing it, or not use it at all.

Transformation of Work Processes[3]

Improvement of operational performance has been investigated particularly in the domain of supply chain management, where the perceived benefits include a reduction in manual errors and improved stock control and management. The IoT will inevitably lead to a redesign of work processes, as organizational responsibilities for control and accountability are changed and redistributed. A shop employee might become responsible for using a system to check the genuineness of an IoT-enabled object and a distant supervisor might become responsible for intervening in case of an incident, which has now suddenly become visible. Difficulties may arise if there is a lack of control capacity, for example if a supervisor is too far away to intervene quickly, or if a conflict arises between new and existing responsibilities.

While deployment of IoT in the workplace could lead to deskilling of workers following automation, they might also be up-skilled as they take over higher level service-oriented tasks. The introduction by libraries of self-service book checkout using RFID means librarians perform fewer routine interactions with customers, and more interactions about problems—which may be regarded by some employees as a drawback. Individuals might also end up feeling less in control and frustrated when using ubiquitous computing or IoT applications if they lack knowledge of how to interact with and use IoT-enriched objects. Workers in one distribution centre perceived an IoT application as unpredictable, because they lacked knowledge of the RFID reading range and how the system functioned. The employees tried to cope with the reading problem with ad hoc solutions that didn't work; some held products behind their back, hoping that their bodies would act as a shield against the reader's field.

Auditing and Liability

Now we are able to monitor previously inaccessible domains through use of technology, we increasingly expect to be able to access information about every aspect of the world that we are interested in. We also assume that information based on digital data is reliable, and increasingly use it as a substitute for other types of information. This informational ubiquity goes hand in hand with societal trends towards flexible control and audit. With its capacity to collect data about work activities and the locations of assets, the IoT promises increased control of complex situations. Companies are also under pressure from clients, insurance companies,

[3] The case studies in this section are from research projects funded by the ETH Research Grant TH -31/06-1 and the EU funded project SToP (Stop Tampering of Products, IST-034144).

and regulatory bodies to become more transparent, and technologies are increasingly being introduced into industrial workplaces to promote health and safety, prevent liability risks, and improve auditing and verification. Where complex sub-contracting and public–private partnerships involve shared responsibilities for work being carried out, companies are increasingly required to provide proof that it has been completed, and to give details on when, by whom, and under what circumstances. Sensors that collect digital data can be deployed in places previously only accessible to non-digital data capture (e.g. based on handwritten records), and thus meet the demand for a specific kind of transparency and control over information.

Workplace Support or Surveillance?

If we move towards new and more flexible types of control that follow us and everything we are interested in, everywhere we go, organizational culture could influence the perception of IoT applications by employees *either* as surveillance tools that enable new regimes of control and audit, *or* as a valued support for their work activities and safety. Or indeed as both at once. There is no conclusive evidence as to the centralization or decentralization effects of IoT applications on organizational structure and power. Increased capabilities for management control, to enforce rules and therefore to control behaviour could point to a centralization of decision making by managers and an increase of their power within organizations. However, increased data collection might not only be used by management to exert increasing power and control over their employees; employees could also use data to hold management to account and substantiate demands for more safety for example.

In summary, the IoT seems set to enable transformation in business processes. Current levels of investment in the technology indicate that a good return is expected by industry in terms of efficiency and productivity. However, the applications implemented so far are mostly concerned with improving current business practice. Many organizations may prefer this incremental and evolutionary (rather than revolutionary) model of innovation, and it remains to be seen how they respond to the more radical, emergent, and perhaps user-led innovation that is likely in the future. A similar evolution was seen in applications deployed in previous generations of the Internet.

Building Smart Cities

In the UK, as in other countries, cities and municipalities face the conflicting challenges of promoting economic growth and ensuring sustainable development. The IoT is widely seen as playing a major part in achieving these efficiency gains, by promoting growth and achieving environmental goals though curbing emissions, discouraging environmentally harmful behaviours, and encouraging energy saving. Several UK cities are currently aiming to be centres of this revolution by developing IoT infrastructures to digitize existing physical infrastructures for energy, water and transport. These city-wide IoT initiatives are often driven by government funding schemes[4] and involve consortia of public and private collaborators, including city councils, utility companies, and digital technology providers. In effect we're seeing the emergence of digital business ecosystems centred around cities. We're also seeing the potential for city-wide technology systems to bring about behavioural change. These new infrastructures embed specific values. They support a normative system for promoting and enforcing sustainable behaviours through information feedback loops, behaviour modification and 'gamification' strategies.[5] They have punish and reward mechanisms to 'nudge' citizens towards the behavioural outcomes desired by those who commission the systems.

Issues of Privacy and Trust

Much has been made of the potential privacy implications of the IoT, and rightly so. Privacy issues arise as a result of the compilation of fine-grained data about the consumption behaviour of individuals and neighbourhoods, and from the creation of predictive models for energy, water and transport usage. It is not difficult to imagine a future city-wide information system that knows where you live, knows when you are home and can predict when you will leave, knows when and how often you watch TV or use your washing machine, knows when and how often you use your car, and can predict where you drive or which bus you are going to take in the morning. It would know this because of sensors in your home and car, and digital traces collected by your digital transport ticket. Opting out of such a systems may not be easy, if it meant non-availability of basic services such as heating or transport, or required paying a premium.

To succeed, public IoT infrastructures require broad public support that can only be achieved through wide-ranging engagement of citizens and measures to help citizens understand the purpose and ramifications of proposed developments. If this is not done early on we can expect resistance by those who will ultimately be affected by these developments. Numerous smart energy projects in the US and Europe have already had to be abandoned because consumers didn't trust the intentions of energy companies when installing smart meters in the home. However, we have seen with the roll-out of Transport for London's Oyster travel card that people can be incentivized to trade in their privacy for certain services, particularly if they have trust (whether deserved or not) in the organization that is perceived to be managing it.

Design of Public IoT Infrastructures

Worryingly, city governments generally lack the expertise to drive the design of public IoT infrastructures, relying instead on the expertise of technology vendors and development companies for much of the design, operation, and maintenance. This lack of expertise in city governments is not surprising given the complexity and novelty of large-scale IoT projects, but it makes it very hard for them to understand the implications of design choices and to ensure that 'their' IoT infrastructures fulfil

[4] Such as the Technology Strategy Board's Future City Demonstrator competition: http://www.innovateuk.org/content/competition/future-cities-demonstrator.ashx

[5] Gamification is the use of game-thinking and game mechanics in a non-game context in order to engage users and solve problems. It can be used in applications and processes to improve (for example) user engagement, ROI, data quality, timeliness, and learning.

basic requirements in terms of public accountability, transparency, openness, and equitable sharing of costs and benefits. It is also very clear that there is a fundamental mismatch between the open, participatory character of the Internet and the closed, proprietary way in which many city IoT projects are approached. Not only was the Internet deliberately designed as a loosely coupled decentralized system (aiding reliability and scalability), its governance structure is similarly decentralized. The institutions that regulate and build the Internet are meritocratic and diverse, and are run by many stakeholders who together decide policies and standardization. However, many of the design and governance choices that have made the Internet such a success are undermined by current vendor-driven IoT projects.

Another area of concern of these city-wide systems relates to the development processes and methods used in their construction. Many of them start with upfront specifications and rely on a detailed delivery plan, the assumption being that the system can be fully envisioned and specified before it is built, and that the key challenge is to minimize project risk and costs. In that sense, many of these projects follow a classic public sector infrastructure development model. This model may be inappropriate given it is unlikely that we can fully specify a city-wide IoT system upfront. Too many of the underlying concepts are still unknown (e.g., what are suitable privacy models that support sharing of personal identifiable information in an ecosystem of private and commercial entities, and that at the same time satisfy end-users' preferences?), and too many of the properties of complex IoT systems are emerging properties (e.g. peer-to-peer surveillance enabled by smart meters) that can only be fully understood after development.

Clearly, the emerging IoT has huge potentials, especially in the context of cities, which face the twin challenges of promoting economic growth while also ensuring sustainable development. In this context the IoT can be considered to be a novel public infrastructure that has the potential to serve the interests of citizens and commercial companies alike. However, current public–private initiatives to develop these infrastructures are in danger of falling short of these requirements, as well as missing project targets. Incremental approaches that value learned experiences over delivery of project specifications are one possible way to address these shortcomings, but they have rarely been tested in the IoT space.[6] Finally, with public interest in these infrastructures comes the requirement to seek solutions that ensure public accountability, transparency, openness, and equitable sharing of costs and benefits. However, these public infrastructures are not neutral, being intended to promote specific values, and should be investigated in the context of its normative system.

[6] Alternative models to the classic infrastructure development model include design approaches for large-scale information systems and infrastructures that prioritize small-scale local solutions and that focus on continuous growing of an installed base. Similar approaches (e.g. lean start-up theory and customer development) have emerged in the software entrepreneurship space, which emphasize an incremental approach to business innovation through repeated, hypothesis-driven experimentation. The underlying technology development processes of lean start-ups are informed by agile development practices, which again provide an alternative model to the delivery-focused infrastructure model.

Governing the Internet of Things

New developments around the IoT will move faster than the relevant law and policy, creating a challenge to governance and policy in this area. The regulatory processes that were 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. Where such data have been collected by a device located in (for example) a weather balloon, the risks to data privacy are likely to be low, but when the data are collected by a device with an inextricable or inferred link to a person, these risks clearly rise. Many of the risks will arise from the use of a persistent identifier that links the data back to the device from which it was collected, and therefore back to an individual.

Some key issues of governance and regulation include:

- Rethinking data protection policy and institutional changes to cope with the scale of the IoT.
- Accountability and liability: increasing or obscuring accountability for failures, data breaches, costs, and responsibilities for failures.
- Governing devices that will know a great deal about their users, and actuators that can initiate a series of actions, such as in response to sensor readings.
- Determining who sets what standards will have major implications for business and industry and national technology-led industrial policies.
- Alignment of local, national, regional, and global practices and policies.

Privacy and Data Protection

Despite growing privacy concerns, privacy is still not holistically regulated or even legally addressed in many countries. Instead, privacy regulation is an international patchwork that fails to establish a common trust framework for the people while often forcing companies to incur a high transaction cost for compliance. In times of rapid and constant technical evolution, regulation often comes too late, lacks practical enforcement mechanisms, and finds itself charged with crippling innovation.

Data minimization. The security of a system is often a starting point when considering the risks to personal data, and includes the confidentiality, availability and integrity of the data as it is collected, recorded or transmitted. However, it is important to remember that data protection means more than just implementing end-to-end encryption or some other technical measure to prevent outsiders intercepting or eavesdropping on a communication. Data minimization is an important data protection concept that is at risk of being forgotten in the increasingly connected digital world, and where problems could result from the generation of large quantities of data that are not necessarily valuable or needed, and that can be misused in ways that lead to invalid inferences. This ties in with the data protection principle that data “shall be adequate, relevant and not excessive” and that it “shall not be kept for longer than is necessary”.

Privacy by design is another important data protection concept in the IoT. Globally integrated, timely and effective privacy protection may become more effective if global industry players, associations or whole sectors commit to institute common privacy procedures and integrate privacy-friendly architectures and defaults into their systems. By embedding privacy-friendly approaches to data collection many potential problems can be avoided; for example, a data collection device might be capable of high-frequency recordings but will only transmit the data in an anonymous or aggregate form, and retain historic data for a short time period. An assessment of the impact on data protection and privacy at the outset of a new project or system (e.g. through a privacy impact assessment, PIA),[7] and the implantation of effective mitigating controls will help to avoid potential areas of concern, yet maintain and realize the potential for innovation predicted by many commentators.

Lessons learned (1): The UK's Smart Metering Programme[8]

Following requirements in the 1996 EU Energy Efficiency Directive, member states are developing programmes to encourage the installation of 'smart' power meters that record much larger quantities of data about power usage than traditional meters. The data can be shared automatically at varying intervals with energy suppliers, grid operators, and price comparison websites. These meters can also reveal a great deal of information about individual household activity, and their impact on privacy has become a high-profile matter of interest to energy and privacy regulators, and to privacy campaigners, journalists, and members of the public. In one significant case, the First Chamber of the Dutch parliament rejected two smart metering bills in 2009 because of privacy concerns, forcing the government to add significant privacy protections to revised bills that were passed in 2011.

Despite the repeated claim by the British government that it would follow 'privacy by design' principles in developing its own smart metering programme, many civil society experts are sceptical about whether this actually happened in practice. A key requirement of privacy by design is that privacy options are considered as early as possible in the development of policies and technologies, however, the May 2007 appraisal of options for the Department for Business barely mentioned privacy, and by the time of the Department of Energy and Climate Change (DECC) May 2009 consultation (which made just one mention), key decisions had already been provisionally made on the system architecture, such as the inclusion of a centralized Data and Communication Company. While such a provider could enforce constraints on the flow of data from meters to networks and suppliers, it would also provide a convenient central point at which other interested parties, such as law enforcement agencies, could access meter data given legislative authority. More privacy-friendly options were not given serious consideration—unlike in Germany, which developed specifications for a home gateway that communicates with all parties and aggregates data according to specific recipient profiles.

[7] Privacy impact assessments are aimed at organizations that are developing projects that might have implications for people's privacy. They help organizations assess and identify any privacy concerns and address them at an early stage, rather than as an (expensive) afterthought. See: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx

[8] This section is drawn from Ian Brown (2013) Britain's Smart Meter Programme: A Case Study in Privacy by Design. International Review of Law, Computers & Technology. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2215646.

Following pressure from the statutory consumer group Consumer Focus, DECC started to pay more attention to privacy issues. Following a further call for evidence in 2011 and a final consultation in 2012, DECC published final plans on data access and privacy for the programme, and an assessment of human rights compatibility. These took note of opinions from the Article 29 Data Protection Working Party, the EC's proposals for reform of the Data Protection Directive and Recommendation on the roll-out of smart meters, recommendations from the European Regulators Group for Electricity and Gas and the European Task Force on Smart Grids, and developments in other member states, the US, Canada and Australia. The British programme ultimately ended up with similar rules to the amended Dutch programme: meter installation is voluntary for customers; energy consumption is measured for billing purposes without specific consent at monthly (Britain) or bimonthly (Netherlands) intervals, and when customers move or change suppliers. More detailed data can be read for specific legal obligations, but explicit consent is needed for half-hourly (Britain) or hourly (Netherlands) readings to be taken for other purposes. While these compromises seem to meet the basic requirements of the Data Protection Directive and European Convention on Human Rights, earlier consideration of more privacy-friendly options might have produced a more protective (and cheaper) system.

Lessons learned (2): Developing a European RFID Privacy Recommendation

In 2009 the European Commission issued its RFID Privacy Recommendation, which established the requirement for industry to come up with a framework for personal data and privacy impact assessments for RFID applications; finally endorsed by the Article 29 Data Protection Working Party in January 2011. The Framework was intended to be a self-regulatory effort by industry, in collaboration with relevant civil society; by avoiding over-regulating the precise dos and don'ts of specific technologies the European regulator hoped that global industry players and sectors would embrace privacy impact assessments (PIA) or comply with self-regulatory frameworks that made sense in their industry context. The road to agreement of the PIA Framework was a rocky one, with industry groups splitting into two competing industry camps and developing separate frameworks that then had to be consolidated.[9] Despite the fact that this competitive approach actually considerably improved the end-result, civil society NGO representatives had no influence on the process (despite the text of the Recommendation) and the PIA Framework has so far not been respected by companies in Europe, because they don't see it as mandatory.

Positive aspects of the process were that the informal working group included many members who had for many years followed the RFID privacy policy process and who were experts on the subject. The gate-keeper role of Art. 29 WP as the entity required to consent to the developed policy instrument also ensured its rigour and

[9] The 18 months of informal political battle is described in Sarah Spiekermann (2011) The RFID PIA—developed by industry, endorsed by regulators. In Privacy Impact Assessment, Springer Law, Governance and Technology Series, Hrsg. David Wright and Paul de Hert.

compliance with European legal standards. Moderation by a respected non-involved outside agency (ENISA) helped to achieve consolidation, and the presence in the working group of civil society stakeholders, security risk assessment experts and academics ensured that the final policy instrument was open to respect privacy issues beyond data protection law, and that it considered the structure of a risk assessment.

Nevertheless, the ‘informal’ status of the working group was suboptimal to create an official piece of self-regulation. The working group was not representative of all member states, and a lot of industries using RFID (e.g. in access control, public transportation, and mobile banking industries) were absent. There was no formal procedure and no true reporting responsibility; the industry representative drafting the initial PIA I Framework was neither legitimized nor respected by working group members. Furthermore, there was almost no room for discussion or compromise in the informal working group that could have led to a joint PIA I Framework. The status of the informal working group was unclear to its members, because it operated in parallel to activities pursued by ETSI, which seemed to hold the official mandate to create the RFID PIA Framework.

The final framework signed by Commissioner Neelie Kroes is not taken seriously by industry in member states, because it is not mandatory, because there are no sanctions for non-compliance, and because many industries felt absent from the negotiating table. It is important to use formal working groups or formally recognized standardization bodies for self-regulation, and to make clear what political impact and status the developed policy instrument will have, what legal sanctions will ensue if industry does not stick to its own rules, and ensure that the sanctions are high enough to incentivize privacy compliance. When creating policy instruments, it is also important to ensure participation from all stakeholders, to follow transparent procedures that are accepted by all members of the group, and to have enough time and room for discussion to compromise on sensitive issues.

Policy Considerations

The IoT will touch on almost every aspect of public policy: education, environment, health, the economy, security (etc.), and involve a number of governance and regulatory challenges. The following points came up during discussion in the seminar:

1. Industry is going ahead anyway: “the train left the station some time ago”. We need a common compass point between government, regulators and industry if we are to avoid a train crash. Industry is putting in huge infrastructure investments, with the expectation of a return; an understanding of their economic incentives is important.

2. We live in a global economy, but (for example) robotics and ecommerce are essentially based in the US. Realistically, European data protection approaches are not going to be adopted in the US, because it is not economic. It is not certain that ethical systems design is a selling point.

3. Who is making the key policy and design decisions? And which of these decisions are being made by unelected people?

4. Data protection considerations need to be incorporated in the design stage. Everyone knows that privacy is important, but how is it handled in practice, if at all? There tends to be a gap between what is said, and what happens in practice. Most privacy violations are not big moral panics, and the collective memory of privacy violations is quite short. Are these systems opt-in or opt-out?

5. Transparency and multi-stakeholder input is important. It is better to hear about problems early in the design process, and you are much more likely to anticipate potential problems if you have a range of inputs. How much civil society input is there in the policy-making process?

7. Who has jurisdiction over information flows, and are current data protection regulations up to the job? How do you regulate something that may be too complex to understand or control in its entirety?

8. Governments are influenced by lobbying as well as by the evidence, particularly if there is a prospect of economic growth and job creation.

9. The EU Digital Agenda Commissioner Nellie Kroes's speech at the Internet of Things Europe conference in November 2012 estimated that the Internet of Things will consist of 50 billion devices, and 'big data' is already pushing the bounds of current data protection law. Are there any aspects about the IoT that are not covered? Will the Information Commissioner's Office have the capacity to deal with all the extra data and future likely breaches?

10. We need to consider the impact of the IoT on the wider society, not just on organizations. The development of domestic uses of IoT based applications suggests a widening scope for concern about privacy, security and resilience.

11. UK Government departments will need more expertise to deal with privacy issues. The role of the Information Commissioner will be crucial, and the capacity to deal with the volume of business a matter for concern. There is currently more sympathy among politicians at the European level for data protection than in the UK or in the US. Given that policy-making on privacy is basically happening at the EU level, lobbying should be concentrated there.

12. The possibility of repersonalising anonymised data using data analytics (which isn't only a problem for the IoT) poses significant challenges to current approaches to the protection of personalised data.

Ways Forward

New developments in computing, and the reconfiguration of industry towards renewable energies, smart grid technologies, and energy positive buildings are expected to play a key role in what has been termed the 'Third Industrial Revolution'.[10] We are still in the early stages of the IoT—essentially still just building the plumbing—and current uses are still very traditional. However, there is likely to be more radical innovation in the future, which will present its own challenges and opportunities. Several points arose consistently throughout the day's discussion:

1. There needs to be more research on real applications, in order to inform policy and practice. Real-world application trials that involve stakeholders (even on a small scale) are needed to develop more realistic scenarios about potential societal changes, and to distinguish the current reality from hype.

2. There needs to be multi-stakeholder involvement in the early design stages of IoT applications and systems. This allows identification of a wider range of issues that should be taken into account (such as privacy), and is an opportunity to involve the future users of the system.

3. There needs to be greater public understanding and discussion of the technology, its potential benefits, and related issues and challenges.

The IoT raises many complex and potentially revolutionary opportunities and issues in a technological environment that is likely to be emergent and unpredictable. How do we improve public understanding of the IoT in order to encourage informed debate? It was felt by the forum participants that the BCS would be well placed to take a leadership role in this challenge, particularly in terms of its missions of enabling the information society and informing public policy.

[10] Jeremy Rifkin (2011) The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the World. Palgrave Macmillan.