Internet of Things Working Group: Report to PPAB

Status of this document and consultation process

The IoTWG was established by PPAB in 2012. Its ToR, adopted in November 2012, set out the following aims and objectives:

Aims

The aim of the WG is to make recommendations to PPAB for BCS policy and activities in relation to the Internet of Things.

Objectives

1. The WG will make recommendations to PPAB aligned with the Institute's mission and informed by its values. These recommendations should inform the public and professional education activities of BCS and inform its communications with government and opinion formers as is necessary for them to be effective.

2. The WG will engage with and seek the views of other groups in the Institute which have an interest in IoT, and the wider membership of BCS.

This document is the IoTWG's report to PPAB, including recommendations for BCS policy and activities. It was the subject of consultation via the policy hub from 2 April to 5 May and subsequent discussion within IoTWG. No comments were made by members via the policy hub.

Outline

Introduction

> *Contrary to Mark Weiser's claim that ubiquitous computing will enable nothing fundamentally new, I believe that ubiquitous computing will enable something fundamentally new, and the main question is: to what extent does it allow for human agency?*
>
> Rob van Kranenburg *The Internet of Things: A critique of ambient technology and the all-seeing network of RFID*[1]

1. The term 'the Internet of Things' has been in use since at least 2002 and concepts of machine to machine and ubiquitous computing for much longer. In the last year or so there has been a rapid growth in its salience as a concept. It has become one of the next big things in the societal application of computing. Governments, including those in China and the UK, have a place for it in their industrial strategies. Research funding, including that of RCUK and the EU, is made available for IoT projects. Major companies too numerous to mention have IoT programmes, and there is a thriving SME sector. The development of technologies which greatly increase the creation and use of data, much of it personal, raises urgent questions about privacy, security and resilience, some of them affecting fundamental rights. On 17 April 2013 the US Federal Trade Commission made a public call for advice on the impact of the Internet of Things on privacy and security.[2] The PPAB's interest is therefore timely, as is the question of how BCS should respond to this phenomenon. In this report, we consider a number of issues which relate to the societal impact of the IoT and recommend how BCS might play a role in furthering public debate, understanding and critique of this next phase of the development of technology and society.

2. Argument over precise definition and novelty of this is not important. Rob van Kranenburg's discussion in terms of the environment becoming the interface is an inciteful generalisation which goes beyond detailed considerations of specific technologies[3]. What is significant is that the transformation of sectors, which is already proceeding in eg process control, supply chain management, health, energy, waste management, will accelerate. It is perhaps easiest to see the IoT as a term for the next major phase of development of the Internet and its further permeation of social and economic processes. It will be a major source of information for data analysis ('big data') and it will be both dependent on and a driver of the spread of cloud computing. It is similarly dependent on and a driver of the further development of mobile computing.

3. There is great scope for marketing and boosterism in this area – and for what Evgeny Morozov describes as *solutionism*, the belief that all social problems are

[1] R. Kranenburg & S. Dodson (2008). 'The internet of things a critique of ambient technology and the all-seeing network of RFID'. http://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf

[2] Federal Trade Commission *FTC Seeks Input on Privacy and Security Implications of the Internet of Things* FTC press release, 17 April 2013 http://www.ftc.gov/opa/2013/04/internetthings.shtm

[3] Op cit p 15

capable of an Internet-based solution[4]. The gap between transformational visions of the future and the messiness of implementing new systems in the real world is significant. We should neither exaggerate the ease of the transformation, nor underestimate the likely long term impact of the IoT. BCS has a role to play in deploying real knowledge of computer science in support of public understanding of what is possible and how it can be achieved.

4. 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, distinctions between the IoT and the Internet are difficult to maintain. 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 and the scale on which it will take place mean that the IoT will have even more serious impacts on privacy and data protection than other ICTs. 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. While the IoT applications deployed so far largely serve familiar purposes, there is likely be more radical, emergent, unpredictable, and user-led innovation in the future, just as we have seen with the Internet. This wave of change thus has both evolutionary and revolutionary aspects.

5. There is no room for doubt that development on this scale is taking place. As was made clear in BCS/OII seminar on IoT in February 2013, this train has left the station.[5] Governments and industry are investing both political and financial capital in the IoT as a pillar of their respective business and economic development strategies.

6. The speed at which the development of domestic systems will take place on a mass scale is less clear, nor is it clear what the real business, economic or social drivers are for the integration of currently siloed systems. We argue here that the development of all these systems brings with it systemic risks which need to be understood, and that the development of domestic systems, and systems which rely on sharing personal data, will put new demands on the ability of ordinary citizens to understand and manage their information environments. The public should not become the passive objects of technologically driven change, and BCS has a role in expressing a professionally informed view of the implications, and the inevitability, of the IoT.

7. In the early development of the Internet there was a lengthy gestation period largely led by academic institutions. The growth of the Internet of Things on the other hand is taking place in the full glare of commercial and state interests. Large corporate investment is at a very high level. Governments are alive to the possibility of harnessing this technology as a driver of economic growth, both through the increased efficiency of existing processes and the creation of new

[4] Evgeny Morozov 'Why social movements should ignore social media', New Republic 5 Feb 2013 http://www.newrepublic.com/article/112189/social-media-doesnt-always-help-social-movements

[5] The report of the seminar is at http://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf. See also 'The Impact of Things', IT Now March 2013 pp 6-9. http://www.bcs.org/upload/pdf/itnow-mar13.pdf

applications and services. We note that government also has responsibility for protecting the privacy and security of the public, and the resilience of critical national infrastructure. Serving the interests of industrial promotion and public safety is more than just a matter of balance. Fundamental rights are engaged[6]. BCS has an important role to play in deploying the knowledge and experience of its members in raising public awareness, stimulating informed debate and lobbying for the proper recognition of the wider interests of the public through consultation on legislation and regulation.

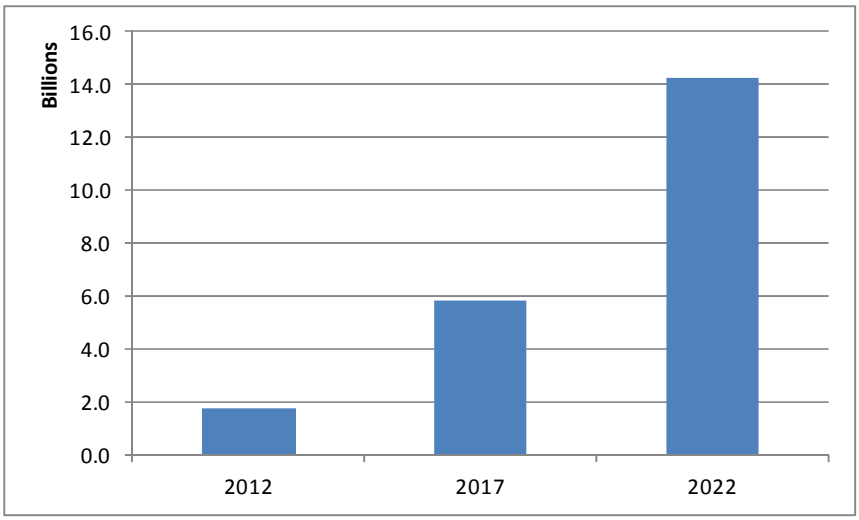
8. We believe that winning public understanding of technologically based change, and maintaining public confidence that privacy can be properly protected, are compatible with healthy economic development. The single major recommendation for PPAB is that BCS should take a lead in public debate around the relevant issues.

[6] There are both utopian and dystopian views on the impact of the Internet of Things on privacy. For the view that IoT means much more pervasive surveillance, see http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google.

Societal impact

9. Evangelists for the IoT envisage a world where all manufactured objects from household appliances to buildings have an identity which can be interacted with by other objects or people. The extent to which this can be realised will be determined partly by social acceptability and also by the discovery of novel uses which create value to society and the economy. Estimates of the scale of this suggest a rapid growth in connectivity in industrial, social and domestic settings. (see fig1).

Figure 1. Estimated number of "smart" devices in households in the OECD



source: OECD 2013[7]

10. The range of possibilities is limited only by our imagination, and of implementation by the market, popular acceptance and regulation by governments. It is therefore not possible to be definitive about the social impacts of the IoT. However, the history of technologies throws up many repeating patterns which can help inform us about both the benefits and the potential risks. These possibilities are best illustrated by examples, rather than at a very abstract level.

11. Many objects today have embedded chips within them that have become normal within society in a relatively short time. An example of this is the car key. Years ago some cars had two keys. One to open and close the doors and another for the engine. Now most cars have a single digital key that acts as a remote control for physical security of the vehicle and can be inserted into the car dashboard. In the last few years, some cars have removed the need to insert the key into a lock and the car can be started as long as the key is within the vehicle. To make the key an IoT device all that is needed is for the key to be given an address. It would also be easy to add a location capability such as GPS. This could be done without the consumer being aware of this and in the volumes of keys made at minimal cost. The advantage of this is that if you lost a key you might be able to find it, in a way that is now possible for lost or stolen tablet devices.

[7] OECD *Building Blocks for Smart Networks* OECD Digital Economy Paper No 215, 2013. http://www.oecd-ilibrary.org/science-and-technology/building-blocks-for-smart-networks_5k4dkhvnzv35-en

All technologies have the potential for use and abuse.

12. The challenge is to minimise the potential for harm while maximising benefits to reduce the chance of society's values leading to a backlash against the technology and the potential benefits being unrealised. If the key in the example could be used for tracking an individual or could be maliciously damaged remotely so that you couldn't drive your car then the social acceptability would be compromised. The wider implications for privacy and security are discussed in more detail in the later sections.

13. A risk is that as a society we become dependent on the capabilities of the IoT and lose resilience. Society faces a general risk from energy security when facing the challenges of climate change. The level of reliability needed from the infrastructure to ensure the viability of the IoT could be a significant problem. The recent Royal Academy of Engineering report on solar flares as part of the UK National Risk Register should be considered in the context of the IoT to test any potential issues of resilience[8].

14. The IoT benefits in Health, Education, Environment, Transport, Energy, Entertainment and other sectors may be significantly different in character and the acceptability be different to various national cultures. For instance, in an ageing society the application of IoT in telecare, telemedicine and assisted living will be radically different to applications in retail.

15. It is likely that the IoT will be accompanied by new business models which will create new legal challenges. For instance, if an individual buys a domestic appliance on a lease arrangement would it be acceptable for the device to be disabled by the supplier if the consumer falls behind on payments? As the IoT matures it may be possible to draw some general principles from the early adopters, but if these principles are assumed before experience and adopted too early it may stifle the innovations which the potential of the IoT could create.

[8] Royal Academy of Engineering *Extreme Space Weather* Feb 2013 www.raeng.org.uk/spaceweathersummary

Standards

16. The effective development of the IoT needs to be supported by the right standards – and there is no shortage of activity in standards bodies to take this forward[9]. Some of the standards effort is necessarily global, but there remains a role for local regulators and standards bodies.

17. There are certain principles which BCS will want to see embedded in standards. We discuss privacy, security and resilience in more detail in later sections of this report. The professional interests of BCS members suggest that BCS should also endorse efforts which promote interoperability. BCS's wider social remit suggests that it should promote the adoption of open standards to avoid supplier domination of particular sectors.

18. BCS doesn't need to be involved directly in standards bodies– nor would it be practicable. However, there may be roles for individual BCS groups which have been engaged in this work to engage with IoT related debates as they emerge.

Recommendation

- BCS should ensure that when there is consultation on standards relating to IOT that it is able to take a view that there is proper representation of what BCS sees as professional and wider public interest

[9] This list does not begin to be exhaustive but it illustrates the range of participants and domains of interest:

> Global standards efforts come under the ITU
> http://www.itu.int/en/ITU-T/techwatch/Pages/internetofthings.aspx
> An example of an industry body in the area is Weightless.
> http://www.weightless.org/news/pr/release/3/en
> For Architecture of the IoT, the EU has been active.
> http://www.iot-a.eu/public
> The IETF definition of the problem statement and concepts required to build an internet of things is at
> http://datatracker.ietf.org/doc/draft-lee-iot-problem-statement/

The Finnish IoT strategy summed up the standards environment as follows in 2011:

> 'Relevant standardization forums for IoT include IETF, IEEE, ETSI, NFC Forum, W3C, and ZigBee Alliance, etc. IETF is responsible for the network-related standards, IEEE, NFC Forum, and ZigBee Alliance standardize the lower-layer protocols, ETSI is defining the IoT concept and architecture, and W3C is starting to standardize semantic access to IoT data. Key IETF working groups include 6LowPAN (IPv6 over Low power WPAN), CoRE (Constrained RESTful Environments), Routing Over Low power and Lossy Networks (ROLL). ETSI has established the Machine-to-Machine (M2M) Technical Committee that is defining an end-to-end architecture for IoT.'
>
> Finnish Strategic Centre for Science, Technology, and Innovation (2011) Internet of Things Strategic Research Agenda

Privacy and ethics

19. It can be argued that the Internet of Things is simply the Internet, so why do we need to consider privacy and ethics in this specific context? The answer is that it represents a dramatic increase in the scope, reach and immediacy of the Internet in relation to people's everyday lives. When data is collected by a multitude of devices that are linked inextricably to individuals, particularly those associated with telemedicine and telecare, but also those connected to people's homes, cars and habits then there are data protection, privacy and ethical issues that demand attention before it is too late.

20. There needs to be a debate among the general public on what is and is not acceptable, starting start with agreement on principles. BCS should adopt and promote a set of principles based on those in the Data Protection Act (DPA) and the Identity Assurance principles for the UK Government ID scheme.

Data Protection Principles for the Internet of Things

i. A 'thing' must only act or communicate for a particular purpose on the authority (or consent) of an individual or entity. The individual or entity must have the legal right to withdraw their authority.

ii. The *purpose(s)* for which a 'thing' may act or communicate must only be those authorised by the individual or entity on whose authority it does so and who has been fully informed of the purpose(s) and of the information that the 'thing' will communicate.

iii. A 'thing' may have multiple identities, depending on the context or purpose for which it is being used. Some identities may be asserted by the manufacturer, provider or operator of the 'thing'; other identities may be specified by the owner or user of the 'thing' (who authorises the use of that identity for the current purpose). In all cases, each identity needs to be sufficiently assured for the purpose for which it is being used. (It should be assumed that a relying party will make a judgement on whether the identity is sufficiently assured.) Multiple identities reduce the ability to associate the identities of 'things' with the identities of people.

iv. The data communicated by a 'thing' to any third party must be the minimum required to achieve the authorised purpose.

v. The individual or entity who authorises a 'thing' to communicate personal data to a 3rd party must have the right to be provided, on request, with copies of all personal data thus communicated. The individual or entity must also have the right for inaccurate data held by a 3rd party to be corrected.

vi. There needs to be a procedure whereby individuals or entities can seek independent resolution of any dispute arising from interpretation or application of the principles above.

vii. Finally, there must be provision for exceptional circumstances, with an onus to show that the proposed action is proportionate, and subject to independent oversight,

Note that these principles apply equally to sensors, virtual things (also known as agents) as to physical 'things'.

Big data mining

21. With the Internet of Things, much more data will be generated and processed, containing unique identifiers which will fall into an uncertain category between personal and anonymous data. In general such data is vulnerable to *intersection attacks* which look for coincidence in time and space to associate data points with known identities of data subjects. Positions which seek to restrict the scope of data protection to so-called 'easily identifiable data' [10] are of concern in this new environment and are likely to lead to an unregulated exploitation of IoT data. This risks damaging privacy by allowing individuals to be identified without their consent, and removes the incentive for sound technical approaches to privacy-by-design in the IoT.

22. The notion of *personal data* implicit in the DPA may be too limited, though this is recognised in the ICO's recently published code of practice for anonymisation. In particular, there is a new threat from big data techniques which enable 're-identification' by the 'joining' of huge sets of data, each of which may, in isolation, be satisfactorily anonymised. As connected devices find their ways into more and more aspects of daily life, there will be a potential explosion of new sources of data which may be subject to such processing.

23. It is the *scale* of evolution of the Internet that gives rise to emerging challenges. In addition, the Internet of Things and the associated mining of the data collected in its operation could ride roughshod over one of the key principles of the DPA, namely data minimisation. This principle is in danger of being forgotten in the increasingly connected digital world.

24. An assessment of the impact on data protection, privacy and ethics at the outset of a new project or system and the implementation of effective mitigating controls will help to avoid potential risks and areas of concern yet maintain and realise the potential for innovation associated with development of the IoT. In this area it is likely that self-regulatory stakeholder driven processes will be needed to complement legal and regulatory provisions. However, this can only happen if there is an informed multi-stakeholder debate on the subject in which BCS should play a leading role.

RFID and NFC

25. RFID tracking is a (hopefully only near-term) nightmare. Most company passes and identity cards only use basic (non-authenticated) RFID technology. This opens up endless possibilities for tracking individuals across all kinds of activities. There seems to be little public awareness of this. Further, it is often simple to clone such passes. Since company passes are, in effect, a condition of employment, the obligation should be on employers to deploy authenticated RFID technology.

26. However, old style RFID tags that were simple, often visible and as easily understood as bar codes are rapidly giving way to much more complicated and sophisticated Near Field Communication (NFC) devices (the emulation of RFID, various tags, secured memory cards and secured micro-controlled tags and cards in mobile devices). These devices have a multitude of different approaches to security (security elements) that are little understood by the average user. The

[10] http://www.statewatch.org/news/2012/jun/eu-council-revised-dp-position-11326-12.pdf

elements are not necessarily compatible with each other and have not usually incorporated privacy and security by design. Add to that the fact that innovation is moving so fast that the uses of NFC for more and more sensitive transactions and applications is happening much faster than deep all-embracing considerations of ethics, privacy and security frameworks for use.

27. More generally, 'appropriate technical measures' (DP Principle 7) must be used to ensure that devices incorporating RFID and other NFC technologies and which can be associated with individuals, directly or indirectly[11], can only be used for the purpose(s) for which they are supplied to the individuals.

Recommendations: privacy and ethics

BCS should

- promote the establishment of a set of Data Protection Principles for the Internet of Things. The seven principles listed above are a starting point for discussion of what these should be.
- promote debate about use of Big Data techniques to process data harvested from the Internet of Things and the risks of de-anonymisation.
- lobby for these issues to be properly reflected in the UK Government's position on data protection regulation.
- promote debate about the use of RFID and NFC technologies which enable tracking of individuals without their knowledge or consent
- promote debate on the ethical dimensions of the applications of the Internet of Things to the private and public lives of citizens.
- advocate strict regulation to prohibit insufficient or inappropriate technical measures for protecting privacy in IoT based systems
- advocate greater attention to privacy engineering for the IoT in the research agenda

[11] The presence in the device of a unique identifier that can be read without prior authentication can enable other parties to track an individual without their knowledge or consent.

Security, safety and complexity

28. The Internet of Things can be seen as an evolution of the Internet and its enabling technologies. There are many examples of capabilities envisaged for the IoT which have been operational for some years. Communities and economies will become increasingly dependent on the infrastructure created by the IoT. The vision is that every gadget in homes, transport, the street, every building will be connected to the Internet, with the potential to pass information, directly or indirectly, between these devices and between them and anything else connected to the Internet. This will create a space in which cyber-criminals, cyber-terrorists and dubious commercial interests have unprecedented opportunities to inflict damage on a wide scale.

29. There is an inevitable tension between the deployment of trillions of 'things', often produced with short-term market pressures as a priority, and the need to maintain the security of the 'things' themselves and the networks they form for their working lifetime – perhaps ten years or more – in the face of evolving threats.

30. The emergent behaviours of independently operated systems of systems are inherently unpredictable. Research is needed into methods and principles for bounding the impacts of emergent behaviours.

31. There are grounds for skepticism that the current technical security architectures will scale to a possible number of devices which is many orders of magnitude greater than at present.

Infeasibility of eliminating vulnerabilities

32. 'Things' are envisaged as *individually* simple. Yet recent experience is that the measures to protect against security threats are themselves becoming ever more complex. It will not be economically feasible formally to prove that every 'Thing' has no vulnerabilities, or to endow it with sophisticated measures in depth to minimise risk.

Lack of assurance of critical components

33. 'Things' are envisaged as (embedded in) articles for consumer use. Inevitably, societies and economies will become increasingly dependent on such 'things' and *networks* of such 'things'. Some of these 'things' will thus be *critical system*[12] components, whose dependability must be assured. In today's markets, function (and fashion) usually take precedence over security and safety in the buying decisions of consumers (and organisations). The costs of assurance, especially of heterogeneous networks, are at odds with both the envisaged scale of the IoT and the rate of new product introduction.

[12] The failure of a critical system has the potential to cause serious harm. Harm may be to the health and safety of individuals; to the interests of a large number of individuals (e.g. their privacy or identity); to the interests of major organisations (e.g. the personal finance sector); or to the interests of a whole society or economy (e.g. delivery of a critical public service).

Emergent behaviours with unintended consequences

34. 'Things' will typically be devices with little or no direct human interaction and yet potentially capable of interacting unsupervised with vast numbers of other unsupervised devices. In a global system of systems, comprising hundreds of billions of interconnected devices, unpredictable emergent behaviours will arise that could have global consequences. There are no proven methodologies for assessing the stability of such systems or estimating the bounds of the consequences of instability. The results of use of automated trading systems in financial services provide just one example of the scale of potential impacts.

Keeping pace with emerging threats

35. Cryptography will be an essential foundation for security. Key management will also be essential - cf. regular bank card re-issue (and security updates). The cryptographic processing power required to reduce the probability of successful attack to a given level is increasing steadily; yet cost pressures on the makers of 'things' will limit the extent to which 'Things', even with online firmware updates, might be capable of keeping pace with this ever-increasing demand.

Increasing scale + increasing dependence = increased risk

36. Scarcely a week goes by without reports of some business-critical system becoming unavailable for many hours, even days - whether in banking, finance (less well publicised), mobile phone operations, transport support, etc. As society becomes more reliant on massive networks, with hugely complex inter-dependencies between 'things' connected via those networks, both the probability and the potential impact of such failures will increase.

37. It is no secret that various parties are probing the vulnerabilities of existing networks, not least those on which Critical National Infrastructure depends. Even more of such networks and even greater reliance on them will, again, increase the risks of such networks being compromised or taken off the air.

Risks and standards for IoT

38. The risks in IoT design are contextually and transactionally sensitive. Successful integration of complex networks of networks is hard to achieve. In designing elements of the IoT, a key success factor may be to exclude as many of the cheap device level components as possible from direct Internet access by using Internet enabled gateways. This is common practice at present when monitoring sensors for such things as irrigation system controls. It could equally be a standard requirement in future designs for monitoring the sensors associated with of an individual's house or all of the telecare sensors for the elderly in their own homes. This ensures fewer paths for attack, albeit introducing single points of failure. However, it is more likely that adequate and sustainable security features would be incorporated on the gateways than on individual 'lowest cost' sensors.

39. BCS also needs to become involved in debates on the emerging standards in the area. There is a great risk of proprietary rather than open standards being developed in this fast moving area in order to get products and concepts to market. It must also be noted that neither the UK nor Europe are lead players in the IoT. China is far more advanced in implementation (particularly in the context

of smart cities) than any other country. There is little clarity on Chinese standards for IoT or their security features. This has the potential to impact on critical national infrastructure as well as the security of systems at all levels.

Recommendations: safety, security and complexity

BCS should

- be involved in ensuring its members and the general public are aware of the security issues in IoT and advising on how to minimise them.
- ensure that Government is aware of the potential for the Internet of Things to become Critical National Infrastructure and advise on how the associated risks should be mitigated.
- participate in debates on the emerging standards in the area of the Internet of Things, particularly those addressing safety and security issues.
- recommend that Government and the Research Councils fund a programme of research into methods and principles to limit the potential impacts of emergent behaviours of massively interconnected networks of independently supplied and operated agents.

Education

The Impact of IoT on Education

40. The impact of the Internet of Things is likely to be revolutionary in all areas of education. This will be a consequence of speed of deployment, ubiquity, global scale, low cost and connectivity of billions of intelligent sensor and actuator devices generating unprecedentedly huge amounts of data. The interconnectivity and cutting across silos will place more demand on hybrid skills throughout ICT and beyond. BCS has an opportunity to be a directional leader so the first educational imperative is for BCS itself to educate itself to ensure that it is ahead of the game and structurally prepared and resourced to play a leading role as IoT applications become more pervasive.

41. At the technical level there will be considerably more focus at the silicon level, bringing BCS and the IET more closely into each other's orbit on a number of issues. BCS might consider potential areas for collaboration with the IET on IoT.

42. The UK has a lead in several IoT areas and there is scope for BCS to encourage educational development and collaborations to maintain that advantage. There will be an accompanying need for educational oversight to ensure maintenance of professionalism and continuous learning and updating during a prolonged disruptive period of change.

43. At the applications level huge quantities of data, especially personal data, will be continually generated to transform the working and social lives of BCS members and the wider community. Existing Internet ethical issues, such as personal data ownership and privacy, will become much more prominent due to scale. We can also expect major implications, still not clear, for education and educational structures at all levels, from business and on-the-job education and training through to universities and schools.

BCS Contribution to debate on Education in schools and universities

Primary and Secondary Education

44. In 2012 BCS played a major role in revisiting the national computer science curriculum. Over the past year around 1 million very low cost Raspberry Pi boards have been sold, allowing cheap Internet connectivity, sensor data collection, collation and analysis. Thousands of children are attending major Raspberry Pi meet-ups out of school hours organised by a few dedicated teachers. BCS could encourage development of such basic IoT skills, especially relating to open-hardware and software, essential for the future and especially address at national level the Catch-22 of target-driven schools being reluctant to teach these skills unless they are on the curriculum.

45. Another potentially fruitful area for developing the British ICT skills base is through 3D printing, which has come down in entry price recently to around £300 following expiry of key patents.

46. There will be scope for BCS to encourage innovation and understanding of IoT in schools through competitions, prizes and public approbation.

47. Teachers will need support to keep up with IoT if their skills are not to be continually outstripped by the technical capabilities of their students. Heads of schools may also need encouraging. BCS should encourage bridge building between IoT professionals and schools.

Further and Higher Education

48. IoT tends to currently be largely a specialist postgraduate topic right now. The Open University has introduced IoT at undergraduate level and is revamping its whole curriculum in this area. It is also looking at revamping its approach to teaching the handling of large amounts of data. There may be scope for BCS through its Academy to embrace such IoT development.

49. BCS should continue to encourage investment in the research agenda. Elsewhere in the report, we refer to the particular needs of research into security and privacy, and for social research.

BCS courses

50. If BCS can keep ahead of the IoT game it will be in a strong position to promote the results of its own learning and use that experience to develop best practice, some sort of certification/accreditation such as an equivalent of the European Computer Driving Licence. BCS might look at the extent to which the Internet of Things introduces novelty and to what extent it may involve existing syllabus content just applied in a different way.

51. There may be new areas emerging that BCS could usefully look at, such as, for example, guidance on conversion from IPv4 to IPv6, or aspects of interoperability standards in an IoT world. It is also worth considering how to structure Continuous Professional Development in such a fast moving area.

Public education and awareness

52. There is scope for BCS to engage in public education and IoT awareness, especially among political and business decision makers. IoT will play a major role in many diverse areas, such as the smart cities of the future, in smart housing, health, transport, energy efficiencies and environmental sustainability. There appears to be much scope for BCS to act as a hub for cross fertilisation of information as well as for the promotion of professionalism for IoT. BCS should prepare its stance and messaging externally and internally for core IoT related issues. These may include personal data, privacy, ethics, transparency, deployment of open source, user rights and sensitivities, security and interoperability.

Recommendations: education

BCS should

- act as a hub for professionalism and continuous development in the IoT.

- promote best practice to business, academia and government in the deployment of IoT applications.
- consider areas of potential collaboration with the IET in education for the IoT.
- review how it supports IoT related educational activity outside school hours as well as within.
- consider competitions to encourage widespread and rapid IoT skills adoption.
- ensure its accreditation of university undergraduate courses keeps abreast of developments in IoT.

The role of Government: research, investment and policy

Challenges for government

53. The Internet of Things presents both opportunities and challenges for the UK government. The UK appears to be well placed in terms of the strength of its research base in this area, with effective collaboration between the research councils and industry. Some UK companies – ARM is a clear example – are well placed to create new business on the back of the implementation of IoT-based solutions. The UK government is committed as well to the exploitation of new technologies, of which IoT is a part, in support of regenerating cities, improving healthcare, reducing emissions and securing energy supply. And so are other governments. Some, notably China, have made much bigger commitments to the creation of smart infrastructure, whether real (e.g. networks) or virtual (standards). There is real pressure in terms of international competitiveness and the pursuit of jobs globally which drives governments to act in this area.

54. At the same time, governments retain responsibility for regulation in order to protect the privacy, security and safety of citizens from such things as data protection violations, cyber attack and the failure of critical infrastructure. These are already difficult issues in the existing state of the Internet. As Bill Dutton has suggested, a certain feature of the development of the IoT is that it will be at least as susceptible to centralised management and control as has been the growth of the Internet itself.

55. We recommend that BCS should bear in mind this combination of roles for government, as promoter, user and regulator, when commenting in consultation exercises on government policy.

A positive agenda

56. PPAB should be aware of the active role which the Government is taking in promoting initiatives relating to the Internet of Things. These include:

    - The place given to IoT and Smart cities as two of five focus areas (the others are cloud computing, big data and eCommerce) in its call for views and evidence on its information economy strategy.[13]

    - The active role in promoting investment in smart cities through the Technology Strategy Board's (TSB) award of smart city status to Glasgow, and the establishment of the future cities catapult[14] in London.

    - TSB's wider promotional role, including its support of infrastructure development and its attention to the SME sector.

    - The research agenda. This is well summarised in report of the TSB's IoT Special Interest Group's on the research programme[15]. We note in particular

[13] http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/79120/bis-13-611-uk-government-information-economy-strategy-call-for-evidence.pdf
[14] http://www.innovateuk.org/content/featured-items/future-cities-catapult-to-be-hosted-in-london.ashx

the emphasis given in this work to the need to support both social and technology research, and to address issues of adoption, social impact, privacy and security.

- The role of public authorities as users or promoters of infrastructure, as in programmes for smart cities, smart grid, smart metering, smart transport and smart health.

- The commitment to computer science education in schools, which is an opportunity for students to develop an understanding of sensor networks, M2M and IoT at a young early age.

Critique

57. There are a number of issues in the UK government 's approach to promoting the development of the IoT which should engage PPAB. It is not clear for example that BCS should adopt a particular position on the argument for whether Government has a role to play in creating new infrastructure for the IoT, although arguments are made that this is desirable in order to establish standards and physical infrastructure. Where BCS considers that there is evidence that the market and existing governance fora cannot create a healthy environment for future, open development of the sector, there is an argument for BCS to add weight to the case for intervention.

58. We have yet to see evidence of effective co-ordination between departmental initiatives. Taken together, the programmes on Smart Cities, Connected Health, Smart Metering, Smart Grid, Smart Transport and others could be the basis for the development of a coordinated effort on standards and infrastructure which would then provide the platform for more innovative developments. It is not apparent that this is envisaged in the information economy strategy or that BIS sees itself as responsible for that degree of cross-departmental coordination. Nor is it clear how the programmes on IoT interact with the programmes which the Cabinet Office is leading on digital delivery of public services. It also appears that some departments have yet to adopt an IoT perspective on the likely development of technology in support of their objectives. We are not aware, for example, of IoT programmes in policing, urban security and justice, although the potential for all of these is considerable.

59. Government's role in sponsoring and regulating the growth of the IoT should be carried out in a responsible manner. The more Government takes the lead in bringing service offerings together, the greater the need for a coherent, cross-sector approach to privacy, security and systems resilience. It is not clear where responsibility for this lies, or that the Information Commissioner's Office will be resourced to deal with the rapidly evolving requirements for data sharing and changing views on what constitutes personal data which are implicit in much of the thinking on IoT. We believe that there should be open debate about concepts around 'total connectedness'. As we have set out in our consideration about resilience and privacy, connectedness comes with costs as well as benefits. These should be properly understood when systems are designed.

---

15 https://connect.innovateuk.org/c/document_library/get_file?p_l_id=2140879&folderId=10756171&name=DLFE-127165.pdf

60. The issue of skills and knowledge needs to be addressed if public bodies are to carry out this role of oversight on behalf of the public. There are grounds for concern that public authorities may not have sufficient breadth and depth in the design of programmes and hence may be unduly reliant on the proposals of suppliers. This is especially the case where programmes are likely to have emergent properties which cannot be defined at the outset. We suggest that there is a role for BCS to play here in developing the awareness and skills of members who are working in these programmes.

Recommendations

- In commenting on Government consultations, BCS should argue for:

    - Intervention where it perceives that the market will not provide a solution in the interests of professional and wider societal interests

    - A coherent approach across government-sponsored programmes in terms of reuse, standards (including standards for privacy, security and resilience), governance and accountability

    - Critical scrutiny of proposals for 'total connectivity' in terms of their strategic impact and benefits

    - Proper regard for professional skills and knowledge on the part of those in public bodies who are sponsoring the development of IoT infrastructure and programmes.

    - Proposals which make for the healthy growth of the SME sector within an environment where major systems integrators and service providers will inevitably play a dominant role.

61. BCS should support the ICO to ensure that it has the capability and capacity to deal with the volume and range of issues generated by the IoT.

BCS structures

62. We have considered how BCS should structure itself in order to address the issues arising from the Internet of Things and, in particular, to take forward the recommendations of this Working group.

63. We believe that there it would be timely for BCS to promote public debate on issues relating to the social impact of IoT, with a view to raising public awareness of these developments. That requires some consolidated action under the auspices of PPAB and delivered by the reconstituted IoTWG and should include:

64. We note first that the field is developing quickly and in many directions. PPAB will wish to take a co-ordinating role in relation to developments particularly those that touch on matters within the scope of BCS's vision and objectives. As the discussions sponsored by this working group have made clear, the Internet of Things is not a single new phenomenon. It may be no more than a marketing concept by origin, but it has come to be an umbrella term which describes a related bundle of developments which are effectively the next generation of the Internet itself. It follows that business related to the IoT is likely to emerge across the board, and most if not all BCS groups should be prepared to respond.

65. PPAB's activities might include:

    - nominating a lead member of PPAB to coordinate activity in this area and to manage a cross-BCS programme
    - adopting IoT as a cross-cutting theme for PPAB in 2013-14
    - requesting groups within BCS to report on how IoT will be part of their agenda in 2013-14, with a view to identifying overlaps
    - strengthening IoT-related topics in the offerings to members, with potentially a role for the Internet SG in leading this
    - identifying regular opportunities to feature articles relating to IoT in BCS publications, including *IT Now*

66. We conclude that there should not be a new, separate IoT group to take responsibility for IoT across the board in BCS. PPAB will nevertheless wish to be satisfied that the process of mainstreaming IoT issues across existing groups is achieved. This suggests that there should be a PPAB lead member for IoT. Experience from previous initiatives – such as that on data guardianship – suggests that there needs to be a resource which can monitor the process of mainstreaming, make the necessary connections and advise PPAB when a sustainable future state has been achieved. With this as an aim, we recommend that IoTWG's life should be extended beyond the submission of this report to PPAB. However, in transforming IoTWG into an implementation body, its composition should be reviewed to ensure that it has sufficient representation from other interested BCS groups to produce and deliver an active plan.

67. Some groups – GRG is an example – will have increasing volumes of IoT related business in future and should be able to access the knowledge needed to

respond effectively. There is also likely to be considerable further business in groups dealing with privacy, security, resilience and ethics emerging from IoT.

Recommendations: BCS structures

- PPAB should take a coordinating role in relation to IoT.
- As IoT cuts across many complementary areas BCS should liaise with relevant bodies such as The Royal Academy of Engineering, The Royal Society, the Digital Policy Alliance (Eurim) and the IET.
- There should be mainstreaming of IoT issues within BCS groups.
- IoTWG should be reconstituted with a remit to implement mainstreaming of the report's recommendations and to support co-ordination of the BCS's activities relating to IoT.
- GRG will need to strengthen its expertise in this field given likely future programmes on which it may be expected to comment.

Summary of recommendations

Standards

- BCS should ensure that when there is consultation on standards relating to IOT that its is able to take a view that there is proper representation of what BCS sees as professional and wider public interests.

Privacy and ethics

BCS should

- promote the establishment of a set of Data Protection Principles for the Internet of Things. The seven principles listed above are a starting point for discussion of what these should be.
- promote debate about use of Big Data techniques to process data harvested from the Internet of Things and the risks of de-anonymisation.
- lobby for these issues to be properly reflected in the UK Government's position on data protection regulation.
- promote debate about the use of RFID and NFC technologies which enable tracking of individuals without their knowledge or consent
- promote debate on the ethical dimensions of the applications of the Internet of Things to the private and public lives of citizens.
- advocate strict regulation to prohibit insufficient or inappropriate technical measures for protecting privacy in IoT based systems
- advocate greater attention to privacy engineering for the IoT in the research agenda

Safety, security and complexity

BCS should

- be involved in ensuring its members and the general public are aware of the security issues in IoT and advising on how to minimise them.
- ensure that Government is aware of the potential for the Internet of Things to become Critical National Infrastructure and advise on how the associated risks should be mitigated.
- participate in debates on the emerging standards in the area of the Internet of Things, particularly those addressing safety and security issues.
- recommend that Government and the Research Councils fund a programme of research into methods and principles to limit the potential impacts of emergent behaviours of massively interconnected networks of independently supplied and operated agents.

Education

BCS should

- act as a hub for professionalism and continuous development in the IoT.
- promote best practice to business, academia and government in the deployment of IoT applications.
- consider areas of potential collaboration with the IET in education for the IoT.
- review how it supports IoT related educational activity outside school hours as well as within.
- consider competitions to encourage widespread and rapid IoT skills adoption.
- ensure its accreditation of university undergraduate courses keeps abreast of developments in IoT.

Research, investment and policy

- In commenting on Government consultations, BCS should argue for:
    - Intervention where it perceives that the market will not provide a solution in the interests of professional and wider societal interests;
    - A coherent approach across government-sponsored programmes in terms of reuse, standards (including standards for privacy, security and resilience), governance and accountability;

  - Critical scrutiny of proposals for 'total connectivity' in terms of their strategic impact and benefits;
  - Proper regard for professional skills and knowledge on the part of those in public bodies who are sponsoring the development of IoT infrastructure and programmes.

- BCS should facilitate the healthy growth of the SME sector within an environment where major systems integrators and service providers will inevitably play a dominant role.
- BCS should support the ICO to ensure that it has the capability and capacity to deal with the volume and range of issues generated by the IoT.

BCS structures

- PPAB should take a coordinating role in relation to IoT.
- There should be mainstreaming of IoT issues within BCS groups.
- IoTWG should be reconstituted with a remit to implement mainstreaming of the report's recommendations.
- GRG will need to strengthen its expertise in this field given likely future programmes on which it may be expected to comment.

Annex: membership of IoTWG

Bacon	Elisabeth	Observer
Bennett*	Louise	
Cory	Therese	Observer
Crump*	Jeremy	Chair
Dean	Jennifer	ISG representative
Eastwood	Christopher	ISG representative
Fish	Ian	
Herbert	Ian	
Holt*	Nic	
Pellinacci	Neil	ISG representative
Riley*	John	
Sparrow	Elizabeth	Observer
Tuck	Karen	BCS HQ
Yapp*	Chris	

* denotes members who took a lead in drafting the report.