



27 November 2008

Our ref: ITF Rep 01/08

Your ref: Consultation on the early challenges regarding the "Internet of Things"

Commission of the European Communities  
Information Society Consultations  
Brussels

By email to [info-iot-europe@ec.europa.eu](mailto:info-iot-europe@ec.europa.eu)

Dear Sirs

### **THE EARLY CHALLENGES REGARDING THE "INTERNET OF THINGS"**

The Institute of Chartered Accountants in England and Wales welcomes the opportunity to comment on the consultation paper on the *early challenges regarding the "Internet of Things"* published by the European Commission in September 2008.

The Institute operates under a Royal Charter, working in the public interest. Its regulation of its members, in particular its responsibilities in respect of auditors, is overseen by the Financial Reporting Council. As a world leading professional accountancy body, the Institute provides leadership and practical support to over 130,000 members in more than 140 countries, working with governments, regulators and industry in order to ensure the highest standards are maintained. The Institute is a founding member of the Global Accounting Alliance with over 700,000 members worldwide.

#### **Economic benefits**

The Commission Staff Working Document on this subject takes it as a given, and does not offer any particular arguments in support of the statement, that the Internet of Things will bring "productivity and efficiency improvements" that "will definitely contribute to improvements in European living standards".

It is true that developments in RFID are likely to improve business operations and thereby to generate business benefits, but the rest of the paper suggests many ways in which its implementation might be quite inefficient, not least if it is insecure (so that people do not wish to use it) or uneconomic. The policy issues in respect of these matters, as identified in the staff paper, are therefore crucial to assuring its success.

It is worth asking the question, therefore, whether the full economic costs associated with resolving these policy issues have been fully factored into the Commission's vision of the future internet. Such costs include not only the developments in infrastructure that will be necessary but the costs of re-engineering social and business activities to achieve the benefits.

## **Public policy issues**

We consider that economic interests, competition rules and data protection are the key issues that need to be addressed. It is absolutely crucial that the public policy interests posed in the staff paper in respect of these matters are fully considered by the governments of the Member States, their data protection authorities and the private sector. In the case of data protection, we also consider that many of the issues that affect personal data are also relevant, from a different point of view, to commercially sensitive data and other forms of business-related IP.

## **Information security**

It is depressing to contemplate an Internet of Things that might simply magnify opportunities for those who wish to distribute spam, to launch denial-of-service attacks, to commit identity theft and to undertake all sorts of other forms of abuse.

This particular technology has particular elements of insecurity arising from the fact that any radio transmission is in principle available to anyone with an appropriate receiver. Nevertheless, the staff paper correctly identifies so many of the other potential problems that will affect an RFID-enabled internet as the same old problems that have affected, and continue to affect, the existing internet.

We do not believe, therefore, that there will be all that many substantially different types of abuse in RFID exploitation, or subsequently in connection with the Internet of Things, from those which already afflict us. The issues will mainly arise from the sheer ubiquity of the technology, which will certainly stimulate a high rate of attempts to abuse it.

There will therefore be a need for the constant development and improvement of security procedures in connection with RFID and its associated technologies. Part of the core expertise of our members is the control, management and use of effective business systems, an important aspect of which is the security of those systems and assurance of their correct operation. We should therefore like to participate, and indeed look forward to continuing our participation, in the UK and more widely in Europe, in discussions about the developing application of security procedures to business systems.

There is likely, for a long time, to be a continuing debate about the extent to which achieving security, privacy and openness in the use of the internet are ultimately compatible. We consider that the basic principle should be that all those with a stake in realising the full potential of the internet (governments, public authorities, the hardware, telecommunications and software industries, information service providers and major commercial users) have to be accountable, through transparent processes and reporting structures, for those aspects of internet security for which they have the greatest elements of responsibility.

The crucial role of governments is to ensure that the allocation of responsibilities is itself transparent, fair and widely accepted. We are a long way from that situation at the moment and we believe that the European Commission has a key role to play in coordinating discussion of the nature and scope of those responsibilities.

## **Competition rules**

It is right to say (section 3.2.5 of the staff paper) that standards should be developed in such a way as to facilitate an open market, but the history of the development of standards in the IT sector suggests that it will be remarkably difficult to achieve this result. The staff paper contains no specific proposals on how it will be achieved. We consider that this is one of the most important issues that need to be addressed as the use of this technology unfolds.

We consider that it is absolutely essential that standards bodies should deal with the matters set out in section 3.2.7 of the staff paper, particularly the issue of achieving genuine inter-operability, otherwise RFID will become either a confusing patchwork of competing and partially incompatible standards or to a large extent a technology under the control of a major monopoly. In either case, the potential benefits that might be achieved from fully inter-operable systems will be significantly reduced.

If RFID and the Internet of Things are manifestly going to benefit the economy, there will be little need to “build awareness” of these developments among entrepreneurs. In particular, if it is already clear that the Internet of Things will “definitely” contribute to economic progress, as stated in the staff paper, it is unclear why there is still an issue about “how to build awareness among ... companies, tag and reader manufacturers ... and developers” whose economic interests would be among the first to be favourably affected by it.

There may possibly be a need to build awareness and trigger action among consumers, although the speed with which consumers have embraced such recent developments as mobile telephones, broadband and Web 2.0 implementations such as social networking, suggest that very little triggering among consumers will be necessary if the price is right. The main problem for governments and regulators may well be keeping up with the speed of developments sufficiently to ensure that regulation is effective.

We should be interested in contributing to the evolving discussion of the extent to which the RFID market ought to be regulated, and the manner of such regulation, both in Europe and globally.

Please contact me should you wish to discuss any of the points raised in this response.

Yours faithfully

A handwritten signature in cursive script that reads "John Court".

John Court  
Head of Faculty of Information Technology  
Direct dial: +44 20 7920 8534  
Email: [john.court@icaew.com](mailto:john.court@icaew.com)