te No. _____

This is to Certify

Registered holder

Virtual authenticity

Trusting our digital credentials allows us to participate confidently in open global transactions to gain access to what we want when we want.

Proving what is real in an increasingly complex world is seen as a significant emerging challenge by many organisations. Although individual companies and even sectors have their own solutions to the problem of verifying what is authentic, there isn't a simple answer to this; nor is there likely to be. While this is a major challenge in the physical world, with the counterfeiting of everything from aircraft parts and pharmaceuticals to clothes and DVDs all on the rise, in the virtual world the problem is even greater. In the varied discussions relating to this topic during the programme, a number of alternative perspectives were shared and a significant proportion of them aligned around the crux of the issue: 'In a world where it is ever easier to make copies, the significance of authenticity is increasing, and gaining ever greater moral value.'

As Diane Coyle highlighted in her initial view on the future of authenticity, we are looking for verification across a number of different levels – from goods to information and from an experience to our identity. In terms of goods, 'fakes are proliferating in the online world. "Fake" music, films and software are sold to the benefit of customers but not of copyright holders.' The challenge here is that the fakes are just as good as the legitimate originals and valuing a fake is not new. As Wendy Schultz commented: 'The arts have a long traditional of valuing copies: Chinese painters traditionally learnt their craft by copying acknowledged masters, with the result that

The internet amplifies the questions of veracity and reliability which have always affected the mass media.

acknowledged masterpieces of Chinese art can themselves be copies.' Likewise, we can today point to the popularity of remixes in the music industry and fan-fiction, where high-quality literature can be created from substandard TV scriptwriting.

In terms of information, 'the internet amplifies the questions of veracity and reliability which have always affected the mass media'. Hence, as one commentator added, 'more people trust Wikipedia than CNN' – even though the latter is a professional news organisation. In one workshop, there was much discussion of how the Obama election campaign had used technology to create a seemingly authentic experience: 'The idea was that people could "get inside" the campaign and make a difference. The impression of being part of the network was certainly there even though the reality was probably different.' Technology, and especially the internet, was used to give people the sense of being closer to the heart of things than would otherwise have been possible, but at the same time it probably also exaggerated their perceived involvement.

Discussions with banks and data companies consistently highlighted the growing need for 'global secure identities' that could be trusted and used everywhere.

A lot of attention focused on how to authenticate identity – particularly online. The big challenge as yet unmet, it was largely agreed, is simply proving who you are in order to access information, purchase a product or a service or even gain entry to a building with excess process and complexity.

"Many of us now have multiple, real and virtual identities, and so can provide various sources of information that, pulled together, can give a rich picture of who we are. The question is, who can and should have access to it?"

As one workshop participant put it, 'authentication involves technological measures of verification … For example, biometric systems and digital rights management are two existing systems of authentication but, to date, and in spite of huge investment, digital rights management has been a complete failure.' Many existing attempts to create systems that work in the virtual space, and cannot be by-passed, have gained support but have not yet developed momentum to bring about global change.

As John Carr pointed out, in some areas, regulation makes identifying people a bigger challenge than it perhaps ought to be: 'For example, in the UK, mobile phones are not sold to people under 18 and so are designed, positioned and bought by parents and given to their children. However, in restricting access to specific content, such as gambling sites and porn, a mobile operator in theory knows whether or not one of its customers is under the age of 18. Some companies have already said that they intend to achieve greater levels of granularity for the sub-18s so that young phone users could soon be stratified as sub-12s, 12–15s, 16–17s etc.' By comparing text patterns, phone usage and download behaviour, the differences between a 12-year-old girl and a 15-year-old boy are clear and steps could be taken to protect them from inappropriate content without having to know their name and address.

However, the big problem is global authenticity: having a system that works within certain national or regional boundaries or within certain sectors but not others is not the answer. Discussions with banks and data companies consistently highlighted the growing need for 'global secure identities' that could be trusted and used everywhere. While government-level authentication of identity via passport, biometric, iris scan or ID card is considered to be largely in hand for the next decade, the more open issue is that of proving who you are and so, for instance, how creditworthy you may be in relation to a specific transaction. This is not just about proving that you are who you say you are when at home using your PC, but doing so when you buy something from France over the mobile internet while you are in India. This second level of authentication of identity is relatively easy to achieve once you have the right data. However, the problem is that the existing data that retailers, utilities and airlines need is currently spread across many other firms: collectively sharing this so that, as a customer, you do not need to keep on providing name, address, date of birth, PIN number and password each time you want something is the core challenge and hence

A 'Google Identity' service or similar that allows us as customers to consolidate all our personal data in one place for sharing with whoever needs access to it to validate who we are could well be in common usage by 2020.

also an opportunity. Initiatives like Open-ID are a step forward here but many see a more integrated approach on the horizon.

Diane Coyle predicts that 'technological solutions will be commonplace in the next few years'. While some take the view that there is a role for the financial services players such as VISA, PayPal, Experian or a similar organisation to become the host of shared personal data to validate virtual authenticity, others see that right now the likely collator will be a company with a broader and established reach – namely

Google. Looking at the impact the company has had in the past decade and the data that it already has on the majority of internet users, some see that a 'Google Identity' service or similar that allows us as customers to consolidate all our personal data in one place for sharing with whoever needs access to it to validate who we are could well be in common usage by 2020.

Whatever organisation makes this happen, many believe that in the course of the next decade the business models that create an efficient and global centralised source of (non-government level) personal data, one that is open and accessible, with the right permissions, will have major impact. It would be a service that reveals only the relevant information needed to prove who you are, where you live or how old you are to the organisation that needs to know. Clearly, there are serious issues about privacy and trust that might jeopardise such an endeavour but the overriding benefit of having one central information point for all may well overcome this problem.
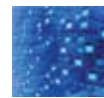
Related insights

Page 125

Page 175

Page 197

Page 235