Aspects of Identity
Yearbook 2012-13

BCS Identity Assurance Working Group

In 2011, BCS, The Chartered Institute for IT, consulted its 70,000 professional members worldwide to determine what they considered to be the most important IT-related issues facing governments in delivering savings, stimulating innovation and enabling ecommerce. One of the key issues was to ensure individuals, not organisations, remain in control of personal information and that individuals should control their identity authentication, which is essential for ecommerce and egovernment to thrive.

Over the last two years, the Identity Assurance Working Group has been examining governance and other issues surrounding identity assurance on the internet. In 2012-13, the group continued the thread of the work reported in the 2011-12 Yearbook through a second series of workshops at UK, European and UN events. The results build on the group's previous findings, continuing to explore the drivers for and proportionality between security, privacy and anonymity on the internet. It also explores practical issues associated with commercialisation of the internet including: improving trust through transparent liability models and contractual frameworks; the value of identity attributes as currency on the internet and other incentives to go online; identity discovery through data attribution; identity theft and fraud. The group once again conclude that there is no possibility of a globally acceptable 'grand scheme' for identity governance, but shared sovereignty, based on no trans-boundary harm is a feasible way forward.
Aspects of Identity

Yearbook 2012–2013
Supporting statements

The DPA (EURIM) continues to support BCS in its drive to improve the governance of identity on the internet through international dialogue at the UN IGF. They are quite right to assert that there will never be a single grand scheme for identity governance on the internet. However, federated commercial contractual models where liability for failure, or recourse for those harmed by failures, is attainable and should be supported. In this context the principle of no trans-boundary harm is key.

The Earl of Erroll, Chair DPA (EURIM)

The issues associated with the management and protection of an individual’s identity on the internet are gradually gaining the recognition that many have been crying out for over the last decade. The work that the BCS Identity Assurance Working Group is progressing is an enabler for the discussions that are taking place worldwide and plays a vital role in providing an articulate, authoritative and independent voice of reason in a world swirling with a host of good intentions. For identity subjects and providers alike wishing to navigate the shark-infested waters of identity assurance, the BCS Aspects of Identity Yearbook 2012–13 offers a much-needed way forward.

Dr David Goodman, Chairman of EEMA,
The European Association for Eidentity and Security

The drive from BCS to develop suitable frameworks for identities on the internet is vitally important. There is a great need to help both individuals and organisations secure their online profiles so that they are not subject to identity theft or fraud and to help ensure future trust in online transactions.

Lesley Cowley, FBCS, OBE
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>vi</td>
</tr>
<tr>
<td>1  Introduction and background</td>
<td>1</td>
</tr>
<tr>
<td>2  Internet landscape</td>
<td>3</td>
</tr>
<tr>
<td>3  Identity-related issues on the internet</td>
<td>5</td>
</tr>
<tr>
<td>The absence of consensus on what security, privacy and anonymity mean in relation to identity on the internet</td>
<td>5</td>
</tr>
<tr>
<td>Anonymity</td>
<td>8</td>
</tr>
<tr>
<td>When do you need a chain of trust and when a network of attributes?</td>
<td>9</td>
</tr>
<tr>
<td>The value of aggregation and data mining associated with ID</td>
<td>10</td>
</tr>
<tr>
<td>Commercial and liability models of internet activity</td>
<td>12</td>
</tr>
<tr>
<td>The context sensitivity of ID</td>
<td>13</td>
</tr>
<tr>
<td>4  Progress and practical ways forward on internet governance</td>
<td>15</td>
</tr>
<tr>
<td>Internet geography</td>
<td>15</td>
</tr>
<tr>
<td>Commercial and liability models to put trust in ID</td>
<td>16</td>
</tr>
<tr>
<td>5  Conclusions</td>
<td>19</td>
</tr>
<tr>
<td>6  Recommendations</td>
<td>21</td>
</tr>
<tr>
<td>Annex 1  Identity authentication, validation and credentials</td>
<td>23</td>
</tr>
<tr>
<td>Annex 2  The IAWG and its activities in 2012 and proposals for 2013</td>
<td>37</td>
</tr>
<tr>
<td>Annex 3  UK IGF: identity governance on the internet – what are the essentials? (March 2012)</td>
<td>38</td>
</tr>
<tr>
<td>Annex 5  EEMA (Paris, June 2012)</td>
<td>49</td>
</tr>
<tr>
<td>Annex 6  Parliament and Internet Conference (London, October 2012)</td>
<td>51</td>
</tr>
<tr>
<td>Annex 7  UN Internet Governance Forum (Baku, November 2012)</td>
<td>52</td>
</tr>
<tr>
<td>Annex 8  BCS EEMA: Thought Leadership seminar on eID enabling business growth – one year on</td>
<td>62</td>
</tr>
</tbody>
</table>
I am delighted that BCS, through its Identity Assurance Working Group, is continuing to promote its policy expertise in the crucial area of electronic credentials.

This Yearbook once again provides an invaluable resource for policy makers who will need to step up their engagement with the issue during 2013–14. Of particular importance will be the UK Government response to the proposal from the European Commission on Electronic Identification and Trust services.

The European Commission proposal aims to encourage the extended use of esignatures in commercial, public service and consumer transactions. It is intended to promote a single European Online Market Place and to encourage consumers to engage in more cross-border transactions. It also aims to boost public sector service delivery through online transactions. However, the final form of the proposal is still unclear because there are many concerns with the detail of the plans.

The prominence of this proposal, together with other draft submissions from the Commission on Data Security and Personal Data Protection, show the intensity of EU policy discussions that will take place in 2013.

I am sure that the data in this Yearbook will guide many of those involved in forthcoming debates and negotiations. We must press ahead with measures to unleash the growth and job creating potential of a fully functional digital single market.

Malcolm Harbour CBE
Member of the European Parliament for the West Midlands, UK
Chairman of the Internal Market and Consumer Protection Committee
1 Introduction and background

In this Yearbook, the BCS Identity Assurance Working Group (IAWG) continues the thread from the work they reported in the BCS Aspects of Identity Yearbook 2011–12. The focus is on practical measures for improving identity governance online including in government, ecommerce and service delivery. It seeks to build on the OECD work in this area.

In 2011, BCS started with a conventional set of key issues associated with electronic identities:

- Citizen’s rights and control of personal data;
- Minimising access and controlling privacy;
- Registration authorities and ID assurance;
- Rights and responsibilities of ID providers;
- The balancing act of security versus privacy.

These issues covered the whole framework for identity governance on the internet and the complex topic of trust in transactions with remote identities: anonymity, pseudo-anonymity (‘pseudonymity’) and attribution. BCS still stands by its main views on these issues, thus they are not repeated here.

The 2011–12 Yearbook was well received. Fifteen hundred copies were distributed and many more downloaded from the BCS website (www.bcs.org/identity). In 2012, workshops were held in the UK (at Infosec and UK IGF), Europe (at EEMA) and internationally via the UN IGF (at the Internet Governance Forum) in Baku (see Annexes) that focused on both the inevitable discussions on security privacy and anonymity on the internet and some practical issues:

- The proportionality between security, privacy and anonymity;
- Identity discovery through data aggregation and data mining;

---

1 The IAWG is a subgroup of the BCS Security Community of Expertise (SCoE) and is made up of members of the SCoE with invited experts from industry and academia.
Aspects of Identity

• The commercialisation of the internet and use of identity attributes as value;
• Legal and commercial frameworks;
• Better use of identity for access to online resources and services.

The key topics of identity assurance (i.e. preventing identity theft and protecting the naive from themselves) still feature heavily. The developing internet landscape is outlined in Section 2. We acknowledge that contradictions and strongly held opposing views exist in relation to such issues as privacy, anonymity, security and data aggregation where these are associated with individual identities, and these are outlined in the first two subsections of Section 3. It is not possible to resolve these issues totally because they are dependent on context and viewpoint, but it is important to understand the conflicting views in order to make progress. The remaining subsections of Section 3 cover many aspects of the remaining four issues above. Section 4 outlines progress and practical ways forward in internet governance that have emerged during the year. Section 5 covers conclusions and Section 6 recommendations.

Annex 1 expands on issues relating to the authentication and verification requirements of different types of transaction. Identity assurance and the use of identity on the internet are increasing in importance as the digital age develops. Not just with the use of identity to access systems, but the use of personal information as a commodity and the need for proportionality between privacy and security.

Annex 2 gives a summary of IAWG activities undertaken in 2012 and proposals for 2013. Annexes 3–8 are summaries of each event that the BCS IAWG attended to which they made formal inputs during 2012 and these have contributed to the thinking in this Yearbook. They are drawn from the published reports and are written by various authors.

The views expressed in this Yearbook do not necessarily reflect the opinions of all members of the IAWG or of BCS. The IAWG members are Louise Bennett, John Bullard, Lizzie Coles-Kemp, Roger Dean, Ian Fish, Steve Marsh, Andy Smith, Toby Stevens, Peter Wenham and David Williams.
The internet has grown enormously from its humble beginnings in the early 1980s. In the last year, as well as millions more people and businesses connecting to the internet, there has been an enormous expansion in the number of ‘things’ connected to the internet. In most countries there has also been an expansion in services being delivered over the internet. Individuals, organisations, computers, smartphones, and ‘things’ all require identifiers and in many situations trusted identities. In the publication *Future Identities*, the UK Government Office for Science speaks of hyper-connectivity and says that in 2011 there were more than 7 billion devices connected to the internet and that numbers are predicted to reach 15 billion by 2015. Sixty per cent of internet users in the UK are now members of a social network site, an increase from only 17 per cent in 2007.

Increased use of the internet for financial transactions and commerce has also resulted in an increase in online identity theft and fraud. In the UK alone 27.6 per cent of adults have been a victim of identity fraud: 4.6 million of them were victims in 2011, losing an average of £481 each. This will continue to be a growing problem as criminals move online, following the money and taking advantage of weak legal protection, especially cross-border.

Globally, each nation is doing different things, developing different laws and regulations and offering different services to their citizens on the internet. In parallel, global businesses and business sectors are developing their own trusted communities to work together on the internet, so there are many privately and publicly developed eID systems in use for defined purposes. These have system-specific operating rules to enable them to work in a trustworthy manner that define the rights and responsibilities of all the parties using them. The sets of rules and procedures have to operate within a plethora of existing national laws and are usually further defined by contracts, service level agreements and arbitration rules. Many of these do not recognise or take into account the international dimension of internet activity.

Another big issue with such identity systems is that they are targeted at the larger customer bases: those that have particular technologies or are IT literate. There is often very little support for the disabled, those with limited IT skills or those whose first language is not one of the top ten.

Global commerce is moving online very fast. The UK leads the way in the world in the percentage of its GDP that is now internet-enabled (7.7 per cent in 2012 according to the UK Office for National Statistics).

The UK Government is one of many that are moving Government services online with its strategy of ‘digital by default’. This poses challenges for individual citizen digital identities that go beyond commercial challenges, including supporting as close to 100 per cent of the UK’s diverse population, with all its types of special needs, as possible. In the commercial world, a business that is selling to consumers requires a business model that encourages consumers to transact online through lower prices, faster responses, higher quality,

differentiated offerings or some other form of enhanced gratification to be successful. Governments might want to interact with citizens who are digitally excluded, financially limited or disinclined to interact online.

Workplace Bring Your Own Device (BYOD) policies are presenting new challenges to all organisations in ensuring they are confident about the identity of the devices, the users of those devices, their access to company data and other security implications.

Last year micro online payments had already grown to importance in some developing countries, where there was no strong pre-digital infrastructure (such as M’pesa in Kenya). These micro-payment systems have become much more widely used this year both in many countries (e.g. Saudi Arabia and Gulf States Blue Card, roll-out of the Indian ID system for distributing rural payments) and with widespread offerings in Europe of ewallets on phones, bank cards (e.g. pay by touch) and special purpose cards.

This internet landscape gives rise to a series of issues related to identity that were explored in the workshops organised by BCS in 2012.

In 2012, we found support from an increasing number of people for our view that digital identity is very complex and both transactionally and culturally sensitive. There are many good articles and research papers being produced on the subject, but one thing is clear, there are many different types of attributes linked to a person, which make up that person’s identity or give it context. Last year we published a basic view of the attributes and how they relate to the person. Figure 2.1 shows an expanded view with more of the online context. What is interesting is that very few of the attributes are actually associated with the core identity of the person and most are context or interaction specific.

Figure 2.1

There is a lot of work going on within the UK Government and elsewhere to define the minimum set of attributes for a core identity and it will be interesting to see what variations emerge on what this set contains.
Five major issues emerged from the workshops during the year. These were:

- Absence of consensus on what security, privacy and anonymity mean in relation to identity on the internet, but with a realisation that privacy and security are often mutually beneficial and the main perceived ‘conflict’ is usually between security and anonymity.

- When do you need a chain of trust and when can a federated network of attributes be used?

- The value of aggregation and data mining associated with identity and the ability to identify someone from data mining results or steal an identity due to the exposure of too many attributes.

- Commercial and liability models of internet activity including the use of identity attributes as a method of payment, transnational commercial agreements and countering crime with commercial models rather than laws.

- The context sensitivity of identity ranging from downloading a brochure to online government services and financial transactions.

These are covered in the following subsections.

**The absence of consensus on what security, privacy and anonymity mean in relation to identity on the internet**

Two thousand and twelve brought some steps towards the provision of electronic identity in the UK and elsewhere, though very limited ‘progress’, if that is the correct word, towards coherent national or global identities. It is worth pausing to consider why this might be and to re-evaluate whether the aim is even desirable.

We have seen, as reported in our 2011–12 Yearbook, and confirmed again in the work of the group this year, that there is very little case for single identities in the personal cyberspace. Individuals have legitimate and desirable reasons to maintain separate ‘ personas’. People behave and interact differently if they are offspring, spouses, parents, work colleagues, managers, members of voluntary organisations or social acquaintances. This is how ‘real life’ works, and there seems no reason why people should be forced to behave differently in cyberspace. While there would be obvious usability advantages in dispensing with the need to remember myriad username and password combinations to access different personal web services, this is a technical issue about authentication mechanisms, and nothing to do with ‘identity’. The absence of any widespread adoption of such a mechanism is a good indication of both the weakness of its economic case and the extent to which it clashes with social practices of multiple personas.
Aspects of Identity

We have also seen illustrations of the wide variety of issues raised around ecommerce. In this space, ‘electronic identity’ is essentially a surrogate for the various properties or attributes that are actually important in a transaction:

• demonstration of an ability to pay;
• authority to order;
• proof of ownership;
• authority to sell;
• guarantees of quality and fitness for purpose of goods and services;
• assurance of delivery and non-repudiation of receipt;
• liability and redress should any of these elements fail.

‘Identity’ is hardly an adequate word to describe this variety of properties, and a single electronic identity is an inadequate surrogate for the assurances required. Again, the absence of widespread adoption of any particular mechanism clearly illustrates the weakness of the economic case in general: rather, a variety of mechanisms needs to be in place for different situations. We should not be in the least surprised that a mechanism for purchasing a house is unlikely to be appropriate for the purchase of a newspaper.

Aside from the economic issues we should also highlight potential disparities between the interests of business and individuals. As has been pithily noted, ‘if you are not paying the full cost of a service you are the product, not the customer’, and this might increasingly be true even if you are paying the full cost. Business might seek to earn value from the exploitation of personal information in ways that work against the interests of individual privacy. People are effectively ‘paying’ for services with their personal information. Even if the business acts ethically, it might be forced by law to divulge information collected on individuals. ‘If you have nothing to hide you have nothing to fear’ might simplistically appeal to middle class, middle-aged, middle England males, but those who have suffered discrimination on grounds of race, gender, sexual orientation, religion or class in some communities in the UK, or in other countries, or at different times, will be less sanguine. The reality is that everyone has something to hide, even if that something is for self protection and perfectly legal.

So this leaves governments as the main drivers for provision of unique electronic identities, arguing that such identities are needed for the online provision of public services or for some loosely defined notion of ‘national security’. This mostly comes back to the ability to prove someone did something beyond reasonable doubt (in court) should they attempt to commit a criminal act online.

The first of these use cases is not dissimilar to that of ecommerce: ‘identity’ is a surrogate for the attributes that are really required for provision of the public service – disability status, employment status, number and ages of dependants, income, vehicle details and so on. Establishing ‘who you really are’ is but a small, and relatively easy, part of gaining assurance of all these attributes. However, linking all these attributes to an identity can cause significant privacy issues. In addition, there are problems of other family members acting for relatives, either benignly because of disabilities or coercively for reasons of control, that make online identity assurance even tougher. Dealing with these effectively would bring concomitantly large information security costs unless privacy is designed in from the start, but this rarely happens. Unlike ecommerce, though, governments most often need to interact with those who might be least well-equipped
to use online services: strong assurance in identity and fraud reduction necessarily take second place to ease of use and increased take-up of services, because the former, not the latter, are the policy drivers for putting services online in the first place.

Finally, we are left with the proposition that widespread strong identities are needed for ‘national security’ reasons. This proposition causes the most ardent divisions in discussions of the role of electronic identities. The fundamental basis for division seems to be around what ‘national security’ might mean, and this question, in turn, depends on the role of the state in relation to the individual. Certainly there are needs to prevent online crime and protect the security of the nation as a whole, but cyberbullying and fraud are criminal acts not national security concerns.

Recent work on Moral Foundations Theory by Jonathan Haidt indicates that views on this relationship might be strongly determined by individual psychology: in essence whether one has a ‘conservative’ (small c) or ‘liberal’ (small l) moral basis. In particular, Haidt suggests moral judgements are made along six axes: care/harm, fairness/cheating, liberty/oppression, loyalty/betrayal, authority/subversion and sanctity/degradation. Conservatives tend to value each property equally, whereas liberals place more value on the first three.

In the national security context, this suggests that conservatives put greater store in the ‘in-group’, in this case the State, and favour measures that preserve the order and authority of State organs. They will feel anxiety that the status quo is under threat, and will wish to adopt measures that reduce perceived threats to the group, whether from criminals, terrorists or other States. Liberals, on the other hand, will focus more on threats to the individual, and this includes perceived threats from the State itself. The measures that conservatives wish to adopt might well be perceived as violations of individual security, and hence as threats to be resisted.

This dichotomy manifests itself starkly in the debate over electronic identity. Those who advocate the enforcement of strong, unique electronic identity for national security purposes emphasise the advantages that anonymity in cyberspace gives those with malicious intent:

- Individuals can bully, stalk and libel; criminals can masquerade as valid customers, as acquaintances, as professional colleagues or as real organisations in order to steal and defraud.
- Terrorists can plan and coordinate atrocities, radicalise others, and undertake cyber attacks on critical infrastructure.
- Activists can damage the online presence of legitimate businesses and publish confidential information.
- Businesses and other States can engage in industrial, military and diplomatic espionage.

All this can be done because anonymity removes accountability and makes the job of law enforcement even harder than it is in the physical world. Online legal instruments are also much weaker due to multiple jurisdictions and an international scope. They argue that forcing use of a single electronic identity, at least for many purposes, makes people more accountable for their online actions and so tempers behaviour, limits the opportunities for criminals to commit fraud, permits the activities of terrorist groups to be tracked more easily, and forces sophisticated State activity to stand out from the background noise. For them, ‘security’ is an ordered society where the State exerts significant control over these malicious elements.

Aspects of Identity

Those who oppose the imposition of electronic identity for national security purposes emphasise the advantages that anonymity in cyberspace gives those with good intent:

- Whistle blowers can expose wrong-doing by powerful individuals or organisations.
- Individuals can partition their lives to limit intrusion by unethical organisations or damage caused by criminals stealing their identities.
- Individuals can escape abusive relationships, hide from criminal or terrorist reprisals, avoid discrimination or seek redemption by starting a new life.
- Activists can organise and campaign against vested interests, giving voice to the otherwise silent majority.
- Governments, particularly democratic governments, can be held to account, their policies challenged and their mistakes or misdeeds held up for all to see.

All this can be done because anonymity protects the weak individual from abuse by the powerful, and provides the transparency that holds the powerful in check. They argue that history is littered with examples where both bad people, and good people with the best of intentions, have done bad things in the name of ‘security’. Forcing use of electronic identity limits individuals’ freedom to challenge and so chills their behaviour, exposes them to greater risk of fraud, abuse and discrimination, and gives States powerful instruments of control. For them ‘security’ is a dynamic society with a healthy interplay among individuals, organisations and the State.

If the Moral Foundations Theory is valid, this dichotomy is not going to be resolved through discussions about electronic identity. These discussions are simply exposing much more fundamental concerns about the nature of societies that people wish to live in. In the meantime, liberals and conservatives will continue to argue across each other because one cannot partly give up the freedom to challenge authority, just as one cannot be partly pregnant.

What we need to discover going forward is where the balance can be agreed and in what contexts the proportionality changes. There will always be bipolar views on this area of online identity, but we must seek to remove the misconceptions and misunderstandings so that the actual arguments can be clearly articulated and discussed.

Anonymity

In the workshops and discussion reported in the 2011–12 Yearbook, the proportionality between privacy and security was discussed extensively. However, this year, possibly because BCS did not run a session at EuroDIG, the proportionality between anonymity and security was less focused.

Privacy actually overlaps with security when seeking to achieve a significant number of objectives related to identity assurance on the internet as discussed above. Those that advocate privacy are in some respects after security for the individual, be that from intrusion into their personal life or preventing targeted actions. Protection of personal data is very much a security issue, especially where large databases hold many millions of personal records. Hence security and privacy are closely intertwined.

Many of the arguments raised against privacy advocates on the internet concern the inability to hold people accountable for their actions. These concerns normally stem from anonymity rather than privacy. Even in EU data protection legislation, there are clauses for law enforcement and national security that take precedence over privacy and this reduces the impact of data protection on true national security objectives.
An anonymous person committing fraud, bullying, terrorism or a serious criminal act over the internet is very difficult to catch and hold accountable for their actions. However, anonymity is reasonable in connection with many transactions, interactions or conversations. It is also needed where there are fears of reprisals, such as under certain regimes. The problem is that in some cases anonymity is used by those who wish to commit acts that are either illegal or immoral without fear of being caught.

In conclusion, we have found the area where proportionality needs most discussion is actually between security and anonymity and we will take this debate forward in 2013. This is shown in Figure 3.1.

Figure 3.1

When do you need a chain of trust and when a network of attributes?

When you are undertaking a transaction, particularly when that transaction is being carried out at a distance, it is important to understand the level of certainty about the identity of the other party that is appropriate for a specific interaction. Are you undertaking a transaction where you need to know a person’s biological identity (so that, for example, the person can be imprisoned if the transaction goes wrong)? Do you need to rely on the classic passport model where you can match the credential for the identity to a chain of trust? Or can you rely, for the transaction in question, on an authorisation model using one or more low assurance sources of identity and associated attributes?

For example, there is a chain of trust involved when you pass through a country’s border control (passport). A passport or some other government authenticated photo ID, such as a driving licence or ID card, is generally used to establish your identity when you are establishing a bank account or undertaking some legal transaction.

Similarly, in a face-to-face purchase using a credit card there is a chain of trust established with the credit card company when the card and appropriate PIN code is entered into a terminal. However, in this case, as with ‘real’ money, the trust is not in the user identity (that the user is who they say they are), but rather that the means to pay is trustworthy.

In many ecommerce transactions, however, it is matter of using a collection of attributes rather than validating a person’s biological identity. Would you, a seller, accept just a credit card number, the associated three-digit security code and delivery address or would you require, in addition, a person’s telephone number and email address? Would you undertake a cross check to ensure the required delivery address matches that of the card holder? Would you also cross check the telephone number or would you use something like the ‘Verified by Visa’ service or ‘MasterCard SecureCode’ service as an alternative or as an additional cross check? While there are verified payment services available that mediate a transaction by hiding a user’s credit card details from a seller, but guaranteeing payment to the seller, these services themselves do not use biological identification of a user. Rather bank, credit card and contact details (home address, email and telephone number) are cross referenced.
As a buyer would you be prepared to give information over and above your credit card number (and delivery address when buying something delivered other than by electronic means) when transacting a purchase? Would you trust the website security certificate as sufficient information to allow you to deal with an internet-based trader or would you do some additional research, such as researching for the company via an internet search engine, reading blogs and forums etc. Or would you resort to using a verified payment service where the trader supports their use?

It is all a matter of the risks you or your organisation are prepared to take. You need to do a risk analysis appropriate to your transaction to inform the level of identity assurance that you want. You will almost certainly want a chain of trust when you are transferring all your money electronically. You will almost certainly be content with a minimal set of attributes to access a free online magazine. In any transaction there will be at least two parties; they both need to accept the level of risk.

Everyone has their own views on this topic. Those views will change over time and be different in different circumstances. It depends on an individual’s risk assessment at the time of the transaction. It is almost a norm for younger people all over the world, and internet users in developing countries, to be happy to trade their identity data attributes for free or cheaper services or goods. This is not the case for many older people or privacy advocates.

The complex subject of identity authentication, verification and credentials are covered more fully in Annex 1.

**The value of aggregation and data mining associated with ID**

The online world increasingly uses a network of attributes to determine identity. As has been described above, when we think about privacy, particularly in relation to commercialisation of the internet and government surveillance and data collection (even with the veil of anonymisation), what many individuals really object to is identity discovery through data aggregation especially where it is used to find out about a person’s preferences and life: the so-called ‘analysis of big data’ without either their knowledge or permission. Yet those same people might be happy to build up a reputation score on auction sites like eBay to ensure they are seen as a trustworthy person to do electronic business with, irrespective of whether they are using their root identity or an ‘anonymous’ eBay identity.

There are many commercial models on the internet. Some services are free or below cost because there is value in the data that customers give up when they use those websites or services. The quid pro quo is usually targeted advertising. As Viviane Reding of the European Commission said on 22 January 2012, ‘Personal data is the currency of today’s digital market’.

We have already said that, ‘if you are not paying the full cost of a service you are the product, not the customer’. It is important that we recognise and accept that truth. You cannot have your cake and eat it. There are costs associated with the internet: if you do not want to pay for services with cash, you must realise that you are paying for it some other way, maybe through your taxes. If you do not pay tax, then through someone else’s taxes, or through your identity and the aggregation of attributes and activities associated with your identity that enable targeted marketing or just advertising. Most young people either do not think about this or they accept it, and it can be a win–win situation. If you do not want your identity attributes to be used and privacy really matters to you, then you can get offline and lose out on some deals offered. Alternatively, there are services available that will help protect your privacy online so that you can access services solely online, or you have to pay for protection through privacy and security enhancing products and processes which minimise your information online (provided the service is still made available to you under these circumstances). Everyone needs to make their own informed choices. These will be culturally and contextually different for each of us, at any point in time.
Interestingly, this is also true over time. Something that is not seen as a privacy issue for someone at college might suddenly become an issue later in life, especially if they go in to a high profile position such as public office. Getting a 16-year-old to think about the implications of their online actions on their future is like getting a 16-year-old to take out a pension. It is sensible, but very hard. As Figure 3.2 shows, personal information disseminates over time into many different areas and once published on the internet it is probable it can never be deleted.⁷

**Figure 3.2**

There are very powerful commercial tools available to mine information about an individual or organisation. Just consider the adverts or suggestions that are made to you the next time you use a social media website or search engine. They will often be tied to your habits. There are open source tools available that will search the whole internet for data on a person or organisation. An internet search engine is itself a very powerful tool and available to anyone with an internet connection.

Concerns about data aggregation and data mining on the internet are likely to increase rather than decrease in the coming years. There is also likely to be pressure for regulation in these areas from liberal voices because of the potential privacy implications. This is another reason why many people will want to use different identities for different activities on the internet to frustrate this data aggregation. Linked with this is the so-called ‘right to be forgotten’ (much discussed in Europe). This might more accurately be described as a right to relative obscurity, as put forward by Woodrow Hartzog of Stanford University.

Identity theft for the purposes of crime is big business and aggregating data from many sources to put together a detailed view of someone’s identity is getting easier. Organised crime has the money to fund the development of sophisticated tools and harness the developments from the open source community.

---

⁷ One IAWG member has found emails he posted to Usenet news groups in 1989 on internet searches.
Commercial and liability models of internet activity

The history of commerce can be viewed as a gradual evolution from initially highly localised activity through increasingly longer distance interactions (e.g. the evolution of the Silk Road). Barely 200 years ago, the speed of international commerce was confined either to the speed of a horse or the speed of a ship, and merchants generally pre-agreed the terms of business between themselves under what we would now recognise as a set of contracts.

The internet is of course the latest and most dramatic accelerant of global commerce. Distance, for intangible goods and services, is now effectively measured by the speed of light, and for tangible goods by the speed of air transport.

The internet recognises neither jurisdictional nor geographic/man-made boundaries, and respects neither neat 'industry sectors' nor public/private sector delineations. It is effectively both ubiquitous and instantaneous. It is effectively limited only by what is considered to be illegal and immoral in all jurisdictions and not what is deemed so on a national level.

So, one of the great questions is how to manage the liability issues (illustrated in Figure 3.3) that accompany such a situation, where many transactions start from a perspective of no identity assurance and are epitomised in the phrase 'on the internet nobody knows you are a dog'. How can trust be maintained/engendered/built, especially at the most fundamental level?

Figure 3.3

We need to recognise that trust and liability go together; you cannot have one without the other. Trust is based on the fact that if, even though it is unlikely, something goes wrong with a transaction, what recourse does one have, who can one look to for liability/redress, where does ‘the buck stop’? What responsibilities are taken on by one party and what entitlements can be expected by the other party?

The default ‘solution’ is that ‘government must step up to fill this void’, but in virtually every nation-state discussion worldwide, it quickly becomes clear that government simply cannot undertake such a role; regardless of whether businesses or the citizen ‘trusts’ their government. Government in itself is not equipped either to take on the liabilities or to accept the obligations associated with vouching for the eidentity of the citizens/businesses falling within its geographic confines.
So, if not government, who then can step up to provide such a blend of trust and liability, and who can manage the associated risks in a ‘joined up’ manner around the world? Who can do so in such a way that governments can be happy that such entities are regulated/can be overseen?

The answer lies in considering what works today and how it works. Take the worldwide ‘payments industry’ as the nearest illustration of an ‘application’ that is both local and global, that crosses all sectors, and that moves (increasingly) in a near instantaneous manner. Consider a payment (such as a credit card payment) as being essentially the movement of bits and bytes of digital information representing (money) value, from one digital identity (namely a bank account) to another digital identity (another bank account) via other trusted digital identities (credit card schemes). We take this largely for granted in our daily lives, we trust it, but we do so substantially because we know that, if anything goes wrong, then there is a pre-established route of recourse usually backed by national legislation. Therefore it does not matter if we buy something on holiday or buy something from another country over the internet, if something goes wrong, national legislation provides protection and recourse.

Almost all steps in commerce (public or private sector) in the internet era require exactly such a capability: the ability for some form of trusted/regulated intermediaries to work together under a common set of pre-agreed terms and conditions spanning both local and global geographies and industry sectors, public or private sector; to underpin the digital identity of each party.

It is a relatively small step to ‘reinvent the relevance of banks’ in performing this role of assuring the eID of its customers.

It was of course the letter of introduction written by one banker addressed to another that effectively enabled the traveller/emigrant to assert his/her identity and trustworthiness as the New World opened up over the past 500 years.

Unfortunately banks and bankers have lost some credibility in the eyes of the general public. To regain this there is a move to separate customer-facing business from investment business and to rebuild trust in the former.

The internet is another such ‘New World’ and it is opening up a great deal quicker, so we need that 21st-century version of the banker or trusted notary to fulfil the role of his predecessors for the ultimate benefit of all: be it for government, for business or for the citizen, it has to be an all-round win.

Commerce, banking and the credit card schemes together offer a proven and trusted method for moving value between points no matter their geographical location. Treating identity as something with value that needs to be asserted and moved in a similar manner starts giving a philosophical view of how eID could work on the internet. Effectively it is not governments that will provide trusted online identity, but rather an array of contractual relationships between commercial organisations and public sector working together to form a federated trust framework. This would need to be backed by national legislation so that the contracts in a particular jurisdiction had the necessary credibility.

The context sensitivity of ID

It is important to remember that every country and cultural group has a different view of identity assurance on the internet. Most of what has been described in the sections above has been written seeing things through the prism of a European democratic society. One of the BCS workshop participants at 2012 UN IGF in Baku said that:
This is a common theme now in many non-Western countries. There are significant differences in the cultural values and social norms across the world that many in the West still do not understand when designing internet services.

So does everyone need an identity, or the same identity, for everything they do? The answer is unambiguously **no**. This was the almost unanimous response from everyone we spoke to from many countries throughout last year and this, the ability to retain anonymity, particularly in countries with repressive regimes, is vital. There is no need to know the biological identity of someone you are playing an online game with. There is every reason for people to want to retain anonymity in some situations, and use more than one identity for different types of transaction. However, it is also agreed that identity assured to some level is needed for some transactions. Most importantly it is needed for buying and selling things. You need to know the counterparty can and will supply the goods or pay the price. You need to know the jurisdiction you are accepting, where liability lies and how you can get redress if things go wrong.

You might also need root identifiers for some things (similar to biological identities for individuals). This is becoming increasingly important as smart homes and online health take off. You want to be certain you are monitoring the intrusion detection in your own home. You want your doctor’s computer to access your blood sugar level and automatically increase the flow of your medication not someone else’s.

So managing your identity online and the identities of things associated with you is becoming a vital skill. How can we manage this effectively on a global scale with billions of people and a trillion things attached to the internet? This needs to be considered both from a technology perspective and from the perspective of cultural responses to the technology. We do not have answers yet, but we are making progress.
It is important to remember that the internet is a common space. There are many ‘sub-spaces’ on the internet, some of them are public and others private. Cyberspace is not flat. There are many separate and overlapping jurisdictions in this multidimensional space. Common spaces work if there is either strong self-regulation or strong external regulation, but you also have the ‘tragedy of the commons’ where no one takes control and some people exploit others. It is important to avoid the latter for commerce on the internet to thrive.

IP addresses are not coincident with any physical space. The internet was originally designed with a topology of IP addresses that did not include any country code address spaces and the geography of the internet does not coincide with any political or jurisdictional geography.

The top-level domain names, that use the UN two-letter country name convention, cannot be taken to represent any national jurisdiction. However, it is common for users to assume that they do. There is an expectation among users that transactions they do over the internet are taking place in the country whose top-level domain name appears in the address. Customers consequently expect any transaction will attract the same levels of legal and consumer protection that they expect if they go into a local physical shop in that country and buy a physical product, whatever these levels of protection might be.

The reality is that just because the internet site you are transacting with uses the top-level domain name of your home country, you do not automatically come under either the applicable law or the jurisdiction of that country (and the two are not the same) for the transaction. In order to know the jurisdiction of the transaction the individual will need to look at the small print. The party you are transacting with might well be located in one country, as a subsidiary of a company in a second country, that is itself incorporated in a third country, under the law of a fourth country with contracts accepting arbitration from a fifth country.

It is very important that both businesses and individuals understand this and its implications if they are to retain trust in the transactions they undertake on the internet. For instance, it is quite easy to register a company in the UK and obtain a .uk domain name, set up a website with this domain and start selling goods. However the servers could be anywhere in the world and only the small print would tell you that it is operating outside the UK Data Protection Act jurisdiction. Equally the whole company could just be a paper entity with no value. Suing the UK registered company would achieve nothing if they have no people or assets in the UK and if the small print states the contractual law of the website is that of another country.

The internet is not hierarchical or pyramidal, like the national and international courts. This makes it non-viable for the International Court of Settlement, as currently structured, to operate on the internet.
Aspects of Identity

Shared sovereignty is perhaps one feasible way forward on the internet. For this to work, a ‘no transboundary harm’ principle is probably the key to progress. There are many cases of voluntary extensions of some sovereign jurisdictions by reciprocal agreements of company contracts or terms of use. In other cases there are reciprocal agreements between individual countries or groups of countries to recognise certain contracts or payments over the internet. For example, this is the case for licensing the resale of some IPR content, such as music and films from specific sites. Some law makers in some countries have sought to extend their jurisdiction over the internet (often resulting in furious controversy). It might be possible to extend the World Trade Organization (WTO) laws into the internet domain, but this is a long way off. Dispute resolution mediated by some large platform owners, who are trusted by the parties involved, such as online auction sites or social media sites, is becoming a popular way forward for consumer rights.

One new group seeking to develop dialogue on this topic is the Internet and Jurisdiction project (www.internetjurisdiction.net) with whom the IAWG have had initial discussions.

**Commercial and liability models to put trust in ID**

There is no single blueprint which can cover all commercial and all liability scenarios that the internet can enable, nor indeed should there be. However, there are some established blueprints that can cover the vast majority of day-to-day transactions, spanning geographies, sectors and multiple applications/uses. It really depends on the end goal. What problems are you trying to solve and, therefore, how big are the potential liabilities and obligations/entitlements that each party might expect to be covered?

Put in another way, the liability issues around the exchange of highly sensitive industrial data/national security issues far outweigh the liabilities for either party in, for example downloading a book or a piece of music. Yet the internet, as a medium, can accommodate both tasks under different commercial/liability models.

In this regard, much space has been devoted to the topic of ‘federated identity’ as being a general purpose transactional foundation stone for trusted internet activity. This is true, but with a caveat that ‘federation’ means different things to different people depending upon the commercial context in which it is used and the liabilities associated with it.

A non-federated model would not work. This can be viewed as having a root trust point with which each group has a trust relationship, sort of a hub and spoke model. Within each group there can be subgroups and even different methods of doing things, as long as the group agrees to the same contractual and policy requirements as all the other groups. This would give a very good option, as shown in Figure 4.1, but on the internet this is not viable because it would require everyone to trust one root entity.

Take two examples of federated identity:

- A loose federation of ‘islands of trust’ comprising essentially a series of bridges (i.e. two party agreements) linking one island to the next along an archipelago; it can work perfectly well, albeit the liabilities/obligations inherited as a transaction hop across from one island to the next might be very different at the end (either greater or smaller) from where they started, with consequent impact upon trust in that transaction.

- Equally one can envisage a series of bridges within a community of islands – every island being connected to every other island directly by a bridge; this can also work, but is clearly not scalable beyond relatively few islands. Such multiple bilateral agreements quickly become unmanageable as more ‘islands’ join and require bilateral agreements among all.
One practical ‘federated solution’ can be drawn from history, modelled upon the way in which federation takes place in the most successful nation-state on Earth over the past 220 years, namely the USA, where an overall Federal Constitution binds all the States of the Union together under a common overall framework (all 50 sign up to exactly the same set of liabilities and obligations, and all 50 then have their own constitutions/frameworks which sit under that federal structure).

As shown in Figure 4.2, this can work as each group signs up to the same set of standards and agreements, which are written and overseen by a membership body rather than being owned by one country or organisation. This web of trust would allow any organisation that was willing to agree contractually to the requirements to offer identity services and be part of the federated community. This would be much like the current online banking systems and credit card systems, which operate quite effectively in the online paradigm.

If this model were to be replicated within the commercial/transactional environment of internet activity using a common industry sector (say regulated financial institutions/banks as the vehicles for this federated structure, given that bank services already have to span geographies, industry sectors, public sector and multiple uses), then one might reasonably suggest that the 80/20 rule will apply; namely that the vast majority of internet activity can be safely enabled under such a framework, while still leaving potentially limitless room for the specialist/very focused applications where such a framework is inappropriate.
Applying the analogy to the internet a step further, in 1789, when the Federal Constitution of the USA was drawn up after the colonial era and the War of Independence, none of the Founding Fathers had any idea of the potential/the extent/the capabilities of the fledgling nation, so they needed a scalable time-proof framework. One can reasonably assert that in the early years of the internet era, we have no real idea of its potential, its reach or its capabilities, but we do know that we need a scalable, durable and common commercial and liability model fit for the majority of transactional internet activity underpinned by strong, trusted authentication. In this regard, history is perhaps a pointer to the future, or as Thomas Jefferson, one of the Founding Fathers and the third President of the USA, famously said, ‘Sometimes it is said that man cannot be trusted with the government of himself. Can he then be trusted with the government of others? [...] Let history answer this question.’
There is agreement among stakeholders that assured identities linked to electronic credentials are needed to underpin many transactions on the internet. The level of assurance varies with the transaction. In some cases, the assurance can be relatively weak. In other cases, it needs to be strong. In particular, relatively strong identity assurance is needed when large sums of money change hands or valuable services and entitlements are provided by either governments or businesses.

The BCS Identity Assurance Working Group (IAWG) considers that while there are some occasions when a government needs an eID that links an individual to their biological identity (e.g. for a passport to assert nationality and its attendant benefits for its bearer), in most cases a less strong level of authentication is sufficient, but one that will hold up in a court of law if the person acts illegally. An individual’s biological identity is seldom essential for commercial transactions per se, although governments might insist that it is used for legal compliance.

The seven key points that came out of this year’s workshops are:

- It is important to understand the different drivers for security, privacy and anonymity, including why and how they pull against each other or overlap. The proportionality between security and anonymity, rather than security and privacy, seems to be most controversial. Security and privacy actually overlap quite considerably and are often mutually reinforcing. There will never be global agreement on proportionality between these, but we should work towards global understanding of different perspectives and be able to accommodate most of them. The great danger here is of people failing to communicate because there is no consensus on definitions and no acceptance of justifiably diverse context-sensitive views on these topics.

- Basing identity for ecommerce on a liability model and using a contractual framework would significantly improve the trust in and commercial use of identity on the internet. Having some means of holding individuals and businesses accountable for their actions and for use of a trusted identity would significantly improve both national and global online commerce. There has to be acceptance that this is different from some legitimate government needs for an identity linked to a unique individual.

- Identity is already used as a form of currency on the internet, with people providing personal information in order to gain free or low cost services in return. This allows the ‘payment’ of those services to come from targeted marketing and other sources. However, many individuals object to ‘identity discovery’ through data aggregation and mining. This in turn can lead to people feeling it is legitimate to withhold information about themselves or lie in responding to requests they feel are unjustified (e.g. mandatory fields on their age, ethnicity or religion being requested before they receive their goods or services). This is especially important where identity discovery is looking for attributes that are not actually identity attributes, but give information about a person’s preferences or life choices.
• People need real incentives to get online and perform commercial activities. In East Africa, M’pesa on mobile phones has done much to help. In the Middle East the card for blue collar workers, originally started in GCC (Gulf Cooperation Council Region) but now moving in to Saudi Arabia, is doing the same. Here a real-world card can act as a digital identity and allow holders to go online and perform commercial transactions. The personal motivation to get online is that it offers something of value to the individual. What individuals consider valuable on the internet will vary enormously. Understanding what individuals value is one key to reducing digital exclusion (as well as availability and affordability). This is a topic that needs further exploration.

• People need help to secure their online profile so that they are not subject to identity theft and fraud. This is already resulting in fear of going online in many countries. Much still needs to be done to help people to understand how to protect their identity and their privacy. It will be necessary to develop training and awareness to help protect the naive from themselves. People should be taught not to put personal information in to websites they do not trust and minimise the personal information they expose on the internet.

• We should not be looking for a grand scheme, but rather small steps and maybe compatible or international standards so that small schemes can interoperate effectively. They each need to be simple and understandable so that they do what is needed and no more. Digital identity is an ongoing piece of work and becoming a critical subject for the success and globalisation of internet commerce. The key is going to be to define a series of practical governance frameworks for different classes of transaction requiring different levels of identity assurance. The UN IGF can play an important part in providing the stage for discussions.

• Shared sovereignty is one feasible way forward for governance on the internet. If this is to work, then a ‘no trans-boundary harm’ principle is the key requirement.
We posed the question at the start of this Yearbook about whether coherent, unique, national or global electronic identities are either feasible or desirable. Our view is that they are not. The vast majority of individuals will always want to adopt different personas in different situations and there is no reason why they should not do so. There is no need to reflect a single physical identity on the internet and doing so might cause more harm than good. However, that does not mean there are no actions that can significantly improve the benefits and opportunities and reduce the downsides and risks in identity governance on the internet by improving identity assurance.

The key to improvement is to accept that parts of the internet will always be the ‘Wild West’. It is important to educate users so that they understand the risks they are taking and know how to protect themselves from them when undertaking any transactions where security, privacy or anonymity are necessary from their individual perspective. This is exactly the same as teaching children how to live safely in society in the physical world, and making sure that everyone learns the rules of the (super) highway. The internet has grown so rapidly in little more than a generation that it is not surprising that this has not yet happened in cyberspace. Identity theft and fraud are of concern to many users. These users need trusted sources of help and advice to access the right protection for their internet use so that they can understand the level of risk to them and reconcile this with what they are willing to accept.

Given this, the BCS IAWG will continue to research identity assurance and increase BCS involvement in both national and international developments in this area. BCS has representation on the International Organization for Standardization (ISO) working groups on Identity Management and Privacy and will continue to input to development of standards in this area on behalf of the membership.

The proportionality between security, privacy and anonymity is still poorly understood and there is much work to do in defining the problem and helping people understand the implications and how these aspects need to work together to benefit the majority. BCS will continue to explore this area during 2013.

Criminals have been much more agile than the police and law enforcement in moving from the physical to the online world. It will take many years (or never) before global enforcement of the law in cyberspace is possible, or even the rules in areas, such as libel, defamation and harassment, catch up and become fit for purpose. Governments and international law enforcement have much to do. Provided that consumer protection and methods of redress for any financial harm can grow in cross-border transactions based on existing models, then risks can be kept low. The key requirement is for the degree of certainty about the identity of individuals, businesses, organisations and things to be related to the value of the transaction.

Governments and commercial enterprises need to build on the successful global schemes that already exist with well-understood liability models in contractual frameworks. These federated high security systems can be trusted. Additional ones can be built for new purposes by new communities of interest. They can be linked together securely where that is desirable.

6 Recommendations

We posed the question at the start of this Yearbook about whether coherent, unique, national or global electronic identities are either feasible or desirable. Our view is that they are not. The vast majority of individuals will always want to adopt different personas in different situations and there is no reason why they should not do so. There is no need to reflect a single physical identity on the internet and doing so might cause more harm than good. However, that does not mean there are no actions that can significantly improve the benefits and opportunities and reduce the downsides and risks in identity governance on the internet by improving identity assurance.

The key to improvement is to accept that parts of the internet will always be the ‘Wild West’. It is important to educate users so that they understand the risks they are taking and know how to protect themselves from them when undertaking any transactions where security, privacy or anonymity are necessary from their individual perspective. This is exactly the same as teaching children how to live safely in society in the physical world, and making sure that everyone learns the rules of the (super) highway. The internet has grown so rapidly in little more than a generation that it is not surprising that this has not yet happened in cyberspace. Identity theft and fraud are of concern to many users. These users need trusted sources of help and advice to access the right protection for their internet use so that they can understand the level of risk to them and reconcile this with what they are willing to accept.

Given this, the BCS IAWG will continue to research identity assurance and increase BCS involvement in both national and international developments in this area. BCS has representation on the International Organization for Standardization (ISO) working groups on Identity Management and Privacy and will continue to input to development of standards in this area on behalf of the membership.

The proportionality between security, privacy and anonymity is still poorly understood and there is much work to do in defining the problem and helping people understand the implications and how these aspects need to work together to benefit the majority. BCS will continue to explore this area during 2013.

Criminals have been much more agile than the police and law enforcement in moving from the physical to the online world. It will take many years (or never) before global enforcement of the law in cyberspace is possible, or even the rules in areas, such as libel, defamation and harassment, catch up and become fit for purpose. Governments and international law enforcement have much to do. Provided that consumer protection and methods of redress for any financial harm can grow in cross-border transactions based on existing models, then risks can be kept low. The key requirement is for the degree of certainty about the identity of individuals, businesses, organisations and things to be related to the value of the transaction.

Governments and commercial enterprises need to build on the successful global schemes that already exist with well-understood liability models in contractual frameworks. These federated high security systems can be trusted. Additional ones can be built for new purposes by new communities of interest. They can be linked together securely where that is desirable.
Aspects of Identity

BCS, and especially the IAWG, need to help develop the understanding in this area and both feed in the input from BCS membership and keep BCS membership informed of developments in this area.

Those individuals who are not online need incentives that are of value to them to persuade them to move online (although some will never move). When individuals have personally attractive incentives they will use the internet to socialise, improve their education and conduct efficient online transactions for goods and services that will reduce their costs. Some of the reduction in costs online will come from sharing their personal information with others. Provided people know this is happening, and consent to it, this can benefit all parties.

People also need to have confidence to engage and to disclose, so we need confidence and trust-building mechanisms. We need service providers to disclose more information about themselves and their information management values and we need service users to have the right and the mechanism to challenge a service provider’s information handling practices.

BCS will not be working to put in place a grand scheme for identity assurance on the internet, but since internet governance must be considered as a global issue, it will be making inputs into the ongoing dialogue on internet governance at UN IGF. BCS intends to work with others to set up a dynamic coalition at UN IGF to take the subject of identity assurance forward.

BCS also intends to become actively involved with the Internet and Jurisdiction project (www.internetjurisdiction.net) and will remain involved with the Digital Policy Alliance work on identity assurance (http://dpalliance.org.uk/) and both national and international standards development (https://standardsdevelopment.bsigroup.com/Home/Committee/50220895).

BCS will continue to take an active involvement with the development of the UK Government identity assurance scheme and will keep a watching brief on the similar system in the USA, through the NSTIC Identity Ecosystem Steering Group (www.idecosystem.org).

BCS will also keep a watching brief on the activities of UNCITRAL (UN Commission on International Trade and Law) – the only universal legal forum for issues associated with electronic commerce.

Finally, digital exclusion remains a concern to the charity. BCS will work to reduce this and find incentives for the digitally excluded to get online to improve their lives and benefit from opportunities on the internet. In this context we will make inputs to citizen panels in the UK through one of the academic members of the IAWG.

BCS will also work with others to write up case studies that demonstrate good practice in identity assurance on the internet.
Identity authentication and verification

An area of confusion that has become apparent is between identity and authentication, so this is discussed in more depth in this Annex (mainly drawing on the legal system in the UK). Identity authentication is the process of checking that someone is who they claim to be and then registering them in a system or giving them an immutable credential, such as a passport.

Authentication of an individual is a measure used to link that individual with certain pre-determined access rights via the provision and verification of credentials. The assurance in the user identity provided by the authentication is normally based on the strength of the link between the user, the credentials and the identity. The link for a strong identity, where the credentials form an immutable link between a person and their established identity is important where high assurance is required, but this is not always necessary online. The problem is then to link the person to the credentials and then be able to validate that link to authenticate the person when they are remote over the internet and operating in an unsupervised environment.

Credentials such as usernames and passwords have many flaws. The biggest is that they can be captured using a keyboard logger or Trojan on the user’s computer. Banks and many other organisations have now moved to more dynamic credentials, which has reduced the risks to their business processes.

Authentication for access control

Access control is just that, it is about controlling access. This includes access to information or even physical access to locations, such as offices. It has two parts: authentication and authorisation. In authentication systems the person is known and their identity already established to the required level dictated by the organisation risk management requirements. Authentication is normally performed in a trusted and/or supervised environment.

What a person can do with the access given to information is then controlled by authorisation to certain levels, which might be linked to payment or role or whatever relationship they have with the organisation, which is not necessarily just about verifying one identity.

Authentication systems usually work by the person being given credentials once their identity has been established. Misuse can then be controlled by policy, which can have a range of enforcement methods from withdrawal of service to being fined. Examples of authentication credentials include smartcard ID and username and password or tokens that can be used for access to email, applications and online services.

Access control is about authentication; granting the right to use an identity which might be an individual account (real identity, alias or persona, group or role) and authorisation: determining the rights a person
has after they have authenticated. Access control is not about initially establishing the identity or verifying the person’s real identity.

**Authentication for service provision (entitlement)**

In order to use a service or prove entitlement, a person needs to be able to establish they have a legitimate claim to that entitlement. Normally a person contacts or is contacted by an organisation and establishes a relationship. This might often be based on a face-to-face meeting, such as opening a bank account. It could also be performed online or via post, though there will normally be physical elements required in the identification process, for example sending a passport to prove identity and a utility bill to show current address etc. This is fine if the organisation is a national one, but really hard to manage if the relationship is being created with an international organisation.

The organisation establishes the identity to meet business risk requirements and often relies on third-party corroboration to verify information provided and claims made. Much of this is done in the physical world of paper today, although more and more checks are performed via interconnected networks and private networks, such as the financial services. Alternatively the organisation can rely on a trusted third party to take all or some of the business risk, such as a retailer and customer relying on a credit card company to take the financial risk.

In a face-to-face environment like a bank or job centre, local processes with human supervision reduce the risk. However, banks do still rely on a passport or driving licence for identity verification, or on possession of a bank card, a hand-written signature and shared secrets for authentication, in many situations.

In the case of a government, the initial establishment of the relationship is often done many years prior to the service provision being required. At the extremes, this can be from the registering of a birth certificate through to registering the death. It is the historical records or footprint in time that is used to assure the identity and establish what the entitlement is, such as the pension or health service treatment and provide the credentials that index the persona to which the person is linked.

**Authentication for legal compliance**

New legislation in the UK, such as the Money Laundering Regulations (2007) and the Anti-terrorism, Crime and Security Act (2001), mean that many organisations (including banks, estate agencies, rental agencies, accountants and solicitors) need to establish a client’s identity, so that if necessary they can provide this information to regulators and law enforcement.

Identification is currently performed with credentials like a passport and utility bill, and in most cases is done via visual verification with a photocopy kept for evidence. Now many of these functions are moving online, but such organisations still need to evidence ‘know your customer’ and as such need a high assurance identity.

There are many other Acts of Parliament that contain a requirement for good identification: these include the Elections Act (2001), which is important for online voting, and the Serious Organised Crime and Police Act (2005).

Identification is also required by companies employing people, especially in sensitive jobs, such as teachers and care workers where the Criminal Records Bureau (CRB) has the task of both identifying the person and checking their history to make sure they are not an inappropriate person for the job. This is often done
Identity registration and verification

Identity verification is different from access control and it is this difference that is one part of the issue being tackled by BCS in the work of the IAWG. Identity registration is something that underpins all other forms of online identity use and authentication.

It is not the claim to entitlement (which might come afterward) nor is it the claim to use a relationship established by the registrar. Identity verification is where a person is linked back to a root identity with a high assurance. This is the activity performed where a relationship is initially being established by the organisation with corroboration of the established identity being provided by a trusted third party. For this discussion, there are two ways of performing identity registration:

- Where the organisation does not have and does not need an ongoing relationship with the person, which is called transient identity.
- Where the organisation wants to establish a relationship and needs to verify initially the person’s identity, which is called the established identity.

With the first type, the organisation might not have an established relationship with the person, but might have a trust relationship with a third party such as a credit card scheme. This is true where it is something like a one-off purchase from an online store.

In the second case there are two processes they can apply. Either the registrar can use a trusted third party to provide a high assurance identity, in which case they might decide to continue using this method, rather than establish their own identity registration or they might establish their own registration for that person.

An organisation would normally establish proof of identity offline with a passport or driving licence in combination with proof of address using a recent utility bill or official letter. However, there are significant issues with this method, mainly around the logistics of either meeting the person face-to-face or getting the documents between the person and the registrar.

Also, checking official documents by untrained people means forged or counterfeit documents can be used. There is a template kit sometimes available on eBay that has the necessary information to print good counterfeit driving licences; the only thing that is needed is a card printer, which costs around £2,500.

Until recently the trusted identity documents, including passport and driving licence did not have any form of electronic interface (other than the MRZ section of a passport) or any supporting infrastructure to use them for online identity verification. This meant they could only be used for visual verification. The new EU biometric passport and some ID cards do offer this electronic interface and therefore provide the opportunity to permit remote authentication services.

Official documents are not as strong at proving identity as many people believe. Obtaining a passport or driving licence depends upon other forms of identity proof, however this is often a birth certificate and a signed photograph that the requestor provides.

A birth certificate is only proof of an event, in this case the birth of a child, not necessarily the birth of the certificate holder. A birth certificate along with a trusted signature can be used to obtain a real passport.
and driving licence, as in the case of Charles Stopford who was in the news for adopting an identity, that of Christopher Buckingham.\footnote{The method he used is often referred to as a Day of the Jackal identity theft after the book in which The Jackal steals the identity of a dead baby.}

The key point is that care must be taken when setting up online identity registration processes to ensure that claims to an identity can be corroborated and verified effectively.

**Authentication methods**

There are different authentication and identity verification methods. The following discusses methods from visual verification through to remote verification of identity so that the reader can gain an appreciation and understanding of how the risks change.

**Face-to-face authentication**

This is where the person is physically present and dealing with another person. Visual verification takes place in a supervised environment, where trusted staff check the credentials presented (e.g. a photo ID) and perform the verification.

Visual verification is normally used where a high assurance in the authentic identity holder is required, such as at a passport control or a bank branch when taking out a large loan. The credential is normally a trusted photo ID like the passport, or something like a bank card with a handwritten signature, that can be checked both logically and physically.

The credential is checked by the person, usually:

- A check of the credential to make sure it is authentic, which can be both a physical check (touch and feel, training in what it should look like, clever anti-counterfeit measures) and/or a logical check (using a device to read information from the credential and compare this with local (offline) or remote (online) information.

- A check of the link between the person and the credential, which is normally a photograph, but could also be a signature (using the world’s best biometric recognition system, the human brain) against the person present.

The key thing with visual verification is that a previously issued credential is being used to link the person with a previously established identity. Visual verification of trusted credentials is often used for identification in order to establish the initial relationship, where the organisation trusts the issuing authority. The question is can this concept be translated to remote identity verification?

**Trusted authentication**

Trusted authentication is where there is trust in the system, including trusted infrastructure and trusted processes. This is normally used for company in-house systems and home access to a local computer.

The important characteristics of trusted authentication are that the person has already been identified and pre-enrolled on the system and the system is under full control of the relying party. This report is
interested in the requirements for the pre-enrolment and providing both capabilities where there is no trusted infrastructure.

**Established system authentication**

An established system is still a trusted system, however it is not fully under the control of the organisation. This is also a form of remote authentication because the person is normally remote from the trust point.

A good example is the ATM network. This is, to all intents, a trusted network, however that trust does not come from a single installation and ownership, but from a myriad of contracts and service level agreements between different organisations that own and run different parts of the ATM networks. This is supported by standards such as EMV. This even crosses international boundaries because ATMs in one country will work with bank cards and be trusted by banks from another.

The relationships between the organisations and the standards on which the systems are based give a high level of assurance in the infrastructure. In the case of the ATM networks, the Electronic Point of Sale (EPOS) networks supporting Chip and PIN authentication and other financial networks such as SWIFTnet, there are processes in place including encryption between end-points that ensure the infrastructure is secure. The trust in these networks is also based on the many years of successful operation.

This assurance between the reader (ATM, EPOS etc.) and the back-office computer means that the decision giving access at the reader can be trusted. This allows a high assurance in any authentication or transaction that takes place. The two main transactions in the example of using bank cards with an ATM or EPOS terminal is the linking of the person to the card with a PIN number and the financial transaction that is recorded at the bank, in which non-repudiation of the transaction is paramount.

The points to be made about established systems are much the same as for trusted authentication. The person is pre-enrolled in the system, and the infrastructure provides the necessary trust to authenticate a person for a specific purpose, linking a person to a persona, not necessarily a real identity.

**Remote authentication of entitlement**

Remote authentication, especially for access control is about allowing the use of a previously established persona, which is getting more common as people use the internet to replace an increasing number of daily activities, but it is not just the internet. Remote authentication also covers the phone, including call centres, where the operator needs to establish who they are talking to. There are also automated call centres, where the system might need to identify the caller.

With the internet, remote authentication is critical. It underpins ecommerce, ebanking and service provision ranging from email to share dealing. In most instances where remote authentication is currently used, there is a risk management decision behind the types of credentials used and the level of authentication required. There is also another mitigation factor, which is insurance. For ecommerce, there is both a good justification for providing a service if the profit is significantly higher than losses from fraud, but if the risk of a serious fraud incident is also covered by insurance, this can also reduce the assurance needed from the authentication processes.

This is one reason why the use of usernames and passwords are still the prevalent method of authentication used on the internet and the handwritten signature is still used on forms. However this is changing, as can be seen by the move to Chip and PIN for credit card purchases.
Remote verification of identity

Remote verification of identity is the particular area that interests the IAWG. This is where an organisation wishes to establish the identity of a person themselves and has no current relationship or only a transient identity is needed, but a high level of assurance is also required. They might wish to offer a service where the true identity is needed due to the risk involved.

Where there is no current relationship there are two choices; either establish the identity for themselves or trust someone else (a trusted third party) who has already established the identity to a high level of assurance.

In the former case, current practice is to establish the identity offline using documents like a passport and corroborated evidence, which in effect is trusting a third party, in this case government. Once the identity is established and the person given a persona with the necessary credentials, the persona can then be used remotely.

In the latter case, there are few current methods that can be used to establish transient identity remotely, even though there is a lot of work in this area. There are only offline methods for trusting an identity previously established by others. This can be done as a one-off, with third-party corroboration of identity, or using a trusted third party with services such as federated identity services to verify the identity each time.

Most current alternatives do not provide a high assurance in the link between the person and credential when authenticating remotely because they do not use biometrics to verify the link between the person and the identity. Even the best of these systems still do not provide proof beyond reasonable doubt that the remote party is the authentic holder of a claimed identity because no commercial solutions currently in wide deployment use biometrics.

Identity assurance

What is identity assurance? Or to phrase this in other ways, when you ask the question, ‘Are you who you claim to be?’; how do you know:

• that the credentials used to link a person to an identity are authentic and valid?

• that the person linked to the credentials used to prove the identity is the legitimate holder of those credentials and that this can be proven beyond reasonable doubt?

• that the person originally linked with the identity and credentials was who they claimed to be and that one or more initial counterfeit credentials were not used to obtain legitimate credentials fraudulently, on which the identity is now based?

For many activities, if a claimed identity is given to anyone without checking its biographical substantiation, then it is pointless having fantastic identity systems because this leads to three fundamental problems:

• The individual could leave a real identity and create a new one and start again to build a social footprint;

• The individual can get multiple identities. This includes having multiple active identity credentials, such as passports in many names;
• The individual could adopt an identity as in *The Day of the Jackal*. For example, an illegal immigrant or terrorist can adopt an identity as their own. This could be the identity of someone who has died, emigrated or in the case of many identity thefts, someone who is still alive.

So the issue that needs to be addressed before an identity is established and credentials issued is ‘who are you?’ There is a good introduction in *Computer Law and Security Report*, however, this mainly links the identity with the birth certificate, which is disputed in another paper on eID as being any good for establishing identity. Therefore something more substantial than just a birth certificate or documents obtained with a birth certificate is required.

The process needs to start with the questions:

• Can I find out anything about this person separate from any claimed identity? For example, by running the photograph and other biometrics through databases to see if the person matches any identity already in existence. Hopefully the only biographical information returned would be for the identity being claimed.

• Does this person have more than one identity and social footprints related to those identities or are they just online personas? If so, can they be brought under one established identity? This can show up as very basic aliases, such as stage names and maiden name.

The answers to these core questions result from a check of that person’s social footprint and biographical history to see where that identity has interacted with society and left a record. This evidence is checked with other organisations to provide (trusted) third-party corroboration of presented evidence. This is getting easier to do online especially with services offered by credit reference agencies and directory services. Even search engines can provide considerable historical information for an identity. For example, a person could be asked several questions, including name, date of birth, addresses for the last 10 years, passport details, driver number, National Insurance number, employment history and other identity related information, such as having bank accounts, insurances and professional memberships. This information can then be checked with various government bodies, professional organisations and commercial organisations to see if the identity exists in their records, for how long it has existed and if there are any major discrepancies between the information provided by the claimant and the information obtained from these databases or between the databases.

The biggest issue with identity assurance is establishing the ID in the first place. Following on from this, the other issue with remote authentication is linking the person to the identity using a credential with any level of assurance.

Once the identity is established the only method of linking a person to that identity in an immutable manner is through the use of biometrics. This can range from simple biometrics, like a photograph to a higher assurance biometric, such as iris pattern or fingerprint. The problem is that biometrics do not really work online and thus, even if used in establishing the identity, are not much use in ongoing authentication.

Once this process is complete, a person should have an established identity with which they are permanently linked via biometrics. This is a high assurance identity because the link should stand up as evidence in court, meeting the critical ‘beyond reasonable doubt’ requirement.

---


Until recently, the trusted identity documents, including passport and driving licence did not have any form of electronic interface or supporting infrastructure to use them for remote identity verification. The new EU passport does offer this electronic interface and therefore provides the opportunity to permit remote verification of identity. However, the infrastructure to use this is not viable for online use yet.

Combinations of credentials can be used to meet many business risk management requirements, balancing cost and usability with security, but there are none that currently work for remote verification of identity.

A high assurance identity is one where a corroborated identity has been established, the person is linked to the identity and this link can be verified beyond reasonable doubt.

**Problem appraisal**

The fundamental problem is this: how to provide high assurance remote verification of identity using some form of credentials, where the process must effectively link the person to the credential, with no supervision of the person and no trusted infrastructure between the person claiming the identity and the person trusting the identity?

The other aspect of remote identity is linking an action to a person. This needs to be done to provide non-repudiation, in other words it needs to be performed in a manner whereby the identity verification and any subsequently linked action will stand scrutiny in court. The normal manner for implementing this is electronic signatures; in Europe, at least, properly implemented electronic signatures have the same meaning in law as handwritten signatures.

Authentication of a user via credentials, for entitlement purposes, in line with business risk is well catered for, as is identity verification in face-to-face (supervised) scenarios. Even authentication for entitlement via remote trusted infrastructure, such as the ATM network is normally secure enough to meet the business requirements; though fake fascias have been successfully added to ATM machines in order to capture information from bank cards (due to lack of supervision), resulting in fraud.

Another aspect of this is the party relying on the decision about the identity verification, might not be the party providing the initial identification and credential provision. The relying party might not even be the party making the decision during identity verification, but might pass this off via a federated identity service to a trusted third party.

Any solution would have to meet the following criteria as a minimum to achieve remote verification of identity:

- Identify the person beyond reasonable doubt and initially link the person to any issued credential using a very strong method.
- Provide a credential (or credentials) with features that would make it improbable to forge or counterfeit them.
- Provide an assured link between the credential and the authentic holder of that credential during subsequent use, that would make it improbable for another person to use the credential without the authentic holders presence or permission.
• Ensure the decision linking the person to the credential is performed in a trusted or high assurance manner, even though there is no supervision of the decision and it is remote from the relying party over an untrusted internet.

• Provide secure remote verification of identity either directly or via a trusted federated identity service provided by a trusted third party.

• Provide a secure link to the credential so that the authentication service can verify the decision linking the person to the credential, and check the credential is authentic and valid, even though there is untrusted infrastructure between the credential and the service.

• Provide electronic signing of actions and transactions, ensuring non-repudiation.

• Have the ability to provide audit and transaction logs as legally admissible evidence.

This leads to a second question: what are the commonalities of remote verification across different communications channels to support different service types?

Nothing is 100 per cent secure. It is not possible or practical to try and implement a 100 per cent guarantee that the person claiming an identity is the authentic identity holder. Even in face-to-face environments only a very high assurance can be obtained. Therefore any solution should be practical, able to withstand challenge by the claimant and prove an identity verification beyond reasonable doubt.

When developing a solution there is specific legislation in most European countries that must be adhered to. In the UK, these include The Data Protection Act, The Human Rights Act and The Disability Discrimination Act that incur implementation requirements. Thus a third question is: what are the legal aspects and requirements of any solution?

A final question can therefore be summarised as: what are the business requirements for implementing a practical solution to provide remote verification of identity, across different communication channels in a consistent manner, beyond reasonable doubt?

**Credentials and their characteristics**

For someone to prove their identity after at least one trusted organisation has established that identity, the person will need to provide some form of credential. The credential could actually be that person. We all recognise people we know without any supplemental information based on historical interaction. This can even translate to the phone, where familiar voices can be recognised. However amazing the human mind is at recognising familiar faces and voices it cannot do the same with strangers, without supporting information or evidence that can be trusted. Where supplemental credentials are needed, that credential and the link to the person will then need to be checked using a trusted process.

Authentication solutions can be built upon three factors or credential types. These factors can be used individually or combined together in solutions to provide increasing levels of assurance about the validity of the credentials and assurance in the link between the person and the credentials. The three credential types are:

• **Something that you have** – Typically this ‘possession’ factor would include keys, cards and tokens. This can include physical keys, such as those used for opening doors or using a car, but can also be logical keys, such as private keys stored on smart cards and USB sticks which are physical tokens.
Aspects of Identity

- **Something that you know** – This ‘knowledge’ factor includes passwords and personal identity numbers (PINs). More complex versions include shared knowledge (e.g. mother’s maiden name or date of birth) or shared secrets (e.g. answers to questions).

- **Something you are** – This ‘physiological’ factor includes physical and unique physiological characteristics normally called biometrics (e.g. fingerprints, iris pattern, voice or facial image).

There are various different benefits, risks and issues with each type of credential. The main issue is that with most credential types used for remote authentication the relying party can only be sure that the person has the correct credential, not that the person is the authentic holder of that credential. This is especially a problem with static credentials such as passwords.

**Characteristics of online channels**

Most authentication solutions available today address authentication on a particular communication channel. For example Chip and PIN is designed for EPOS and ATM, but could not be used over the internet; tokens, one-time passwords etc. are designed for computer networks; shared secrets are most common for voice connections to call centres, but can also be used on the internet.

The main characteristics of online channels are that the person uses a computer to connect to the internet and then to the relevant website of the organisation they wish to communicate with.

Important points to note are that the computer being used might not be the personal computer of the identity user. It might be in a cybercafé, a hotel room or at work. It might not even be a standard computer, it could quite easily be a PDA, tablet or smartphone.

Even with a computer, the operating system (OS) could be Microsoft Windows, Unix or MacOS. The only assumption that can be made with the internet today is that the computing platform has a web browser and is able to work with standard websites, including support for active content, such as Java. Any solution would therefore have to be OS and platform independent and could only rely on the human–computer interface being a basic browser with scripting support.

Any global identity solution would need to be based on standards and standard protocols, even though many different commercial solutions could be used to achieve the same function. It could not restrict the platform, network infrastructure or make assumptions about the user’s skills. This alone makes any identity solution or credential method very hard to develop.

**Service types**

Having defined the channels, it is necessary to define the operational tasks that these channels might be used for in order to provide services remotely. Each service that could possibly be provided is not really relevant to this discussion, so the services have been grouped into categories for which the interest is in the characteristics of authentication required for these services and whether one solution can support all of them. The services fall into four main categories:

- application (new customer, new service);
- transactional (where assurance is needed for a single transaction);
• maintenance (changes, updates, removal);

• enquiries (usage, subject access, lost/damaged/stolen).

Each of these is covered in the following paragraphs.

Application
Application represents scenarios where an individual is remote to the relying party and might not have any current relationship with them. Where there is no current relationship, the person might be applying to create a relationship, which could be for many reasons, examples include:

• applying to an ecommerce website to set up an account in order to purchase from them – this might be to meet legal requirements on proof of identity or obtain a level of assurance where large value transactions are taking place;

• applying to a government department for services or benefits to which they are entitled – here the identity is paramount to proving entitlement to the benefit or service and needs to be checked in order to determine what level of entitlement is correct;

• applying to a professional organisation for membership or government for an identity document or service – here identity is needed both to check the entitlement, but also to corroborate other relationships that might be needed to verify the application.

This is likely to include two main activities in scope for remote verification, though there will be others that are less relevant to this discussion:

• One-time completion of application forms where the provision of identity information is required in the form. There might be the requirement to prove identity before getting a quote or where the identity might be checked later offline (e.g. a mortgage application).

• Initial establishment of the ‘relationship’ or ‘persona’ such that further transactions/services can be performed within that relationship. This is where no previous relationship exists and a person is applying to establish a relationship (e.g. The Child Trust Fund). Once activated, the claimant can gain access using credentials provided by the registering organisation, although if the remote authentication is easy to use, the organisation might just set up their own relationship linked to the user’s current credential.

These scenarios typically ‘establish’ a single request for service or a single request for an ongoing relationship which the relying party can assess and approve.

One of the biggest risks here, both from an identity theft and privacy viewpoint is that whenever someone completes online forms they should make sure it is done on a trusted computer. Filling in forms with lots of personal information in a cybercafé or on an untrusted computer is very risky. A keyboard logger on the machine would be able to capture all of the personal information entered, which could in some cases give criminals everything they need to steal or misuse that identity.

BCS recommends that all home computers are properly patched and run a good internet security package with a personal firewall and an up-to-date antivirus product before personal details are exposed by filling in online forms.
Aspects of Identity

Transactional
Transactions and signing represents scenarios where an individual either already has an established identity or relationship with the relying party or wishes to undertake mainstream transaction as a one off.

The oldest and most common form of transactional processes are those involving a handwritten signature and paper, such as signing a contract or a cheque. However, this is moving more and more into the digital arena, with certain types of electronic signatures now having the same meaning under law as handwritten signatures (e.g. in the UK, The Electronic Signatures Regulations 2002, Statutory Instrument 318).

This gives two types of transactional process:

- There might be the requirement to prove identity in order to gain access to an entitlement, but where no further relationship will be established. This could, for example, include purchasing age restricted goods or passport control at a border.

- Completion of a transaction of high value or high risk, where there is a business need to ensure that the authentic account holder is authorising the transaction. For example, most ebank transactions could use the standard credentials to provide an authentication; but for transactions over a certain value a higher assurance in the identity might be needed.

Another example of a transactional service is evoting, where the requirement is to ensure that any given person is not only entitled to vote, but is also restricted to casting only one vote, even if the requirement is for the subsequent voting process to be anonymous.

Maintenance
Maintenance represents a scenario set where there is already an established relationship and underlying information about the person is known to the relying party. The requirement is that the information can be changed directly by an authenticated person.

Allowing someone to change certain information on a bank account, such as contact phone number might not be a high risk, so could be done with current authentication methods. However, currently it is not possible to change things like the name on the account without a visit to the bank and proof of identity being given using a passport or driving licence, at least not with highly reputable banks that wish to retain their reputation.

With a high assurance identity it could be possible to allow customers to change details like address and women to change their surname via ebanking, thus reducing maintenance footfall in bank branches.

Enquiries
Compliance with the UK’s Data Protection Act and Human Rights Act (especially the right to privacy and family life) means that there are significant restrictions on the type and level of personal information that can be given out. Every person has the right to see the information an organisation holds on them in electronic filing systems (this is called a subject access request), but how does the organisation know that the requestor is the actual person to whom that information belongs?

In most instances the person has to send in a request and pay a small fee, then the information is posted to the address the organisation has on file. It is currently too high risk for many organisations to make such information available via a remote communications channel. However, a high assurance remote identity might be even more secure than the current methods of post to the address on file and the information could be provided online, reducing cost and inconvenience.
There is limited risk in order to confirm simple information such as bank balance. However, being able to confirm the results of a medical test would pose a much higher risk. To be able to offer enquiries in higher risk areas via remote methods would need a very high assurance in the identity of the person making the enquiry.

All of the service types have the same requirement for high assurance identification prior to granting access to a service, this can either be to establish a relationship which will use other credentials or to perform a transient identification where no relationship will be established.

**Legal aspects**

If a solution is to be usable and in any way relied upon, it will need to address a number of legal aspects in order to provide remote verification of identity, not least of which are liability and non-repudiation.

**Theft and identity theft**

The first aspect with a legal agenda is that of actually prosecuting any action that takes place in enforcing policy. This includes theft, identity theft, fraud and breach of contract.

Theft would be covered under normal criminal law, which addresses the theft of physical things, such as tokens and ID cards. Importantly, theft does not cover the misappropriation of intangible assets such as usernames and passwords. In the UK, this is dealt with by another piece of legislation, The Computer Misuse Act (1990), which covers misuse of electronic credentials.

Fraud and misuse of identity are also covered in different aspects by various pieces of legislation, though it is not currently illegal to have multiple identities and in fact is a common law right. There are specific offences for fraudulent use of and obtaining identity. However, committing fraud is also a criminal act under various legislation including The Serious Organised Crime and Police Act (2005) and The Social Security Fraud Act (2001).

Aspects of forgery and counterfeiting (e.g. the use of counterfeit identity documents) are also covered under The Forgery and Counterfeiting Act (1981), though in a broad sense.

**Evidence**

The critical aspect of all the above is the ability to provide evidence that can prove to a court beyond reasonable doubt that a person committed the claimed act. Evidence provision is fundamental to enforcement and non-repudiation. Therefore any system must support the gathering, storage and handling of information that can be used as evidence.

Accounting information, audit trails and monitoring systems are necessary for supporting the provision of evidence; however, it does not matter how detailed the audit trails are, unless they can link the action to the person, not just the claimed identity, they are useless in a prosecution.

Proving those actions and linking them to a person is very difficult in the virtual world of digital forensics and electronic evidence with remote actions using intangible assets, but online commerce and the whole funding of the internet ecosystem is dependent on this to some extent.

The first piece of legislation in the UK to address the issue of electronic crime was The Computer Misuse Act (1990). This details the crimes that can be committed and, in part, the evidence required to prove such
Aspects of Identity

crimes. New legislation might be required to update the Act and improve legal protection for use of online identity.

**Electronic signatures**

Even when a person has been linked to an identity remotely, there needs to be some method of tying the actions that take place to the identity. The method supported under law is electronic signatures. There are two pieces of legislation within the UK:

- The European Directive 1999/93/EC;

In order for the legislation to be effective, any solution would have to provide an advanced electronic signature as defined by legislation. This means that the electronic signature produced by using the solution would normally have the same meaning under law as a handwritten signature. Any transactions signed using the remote identity would then also have the same meaning.

Implementing this functionality will provide non-repudiation and legally admissible signatures, so it is therefore a requirement that any remote authentication solution should provide for advanced electronic signatures.

**Disability discrimination**

The next legal aspect is one that is often overlooked, but it is one that is very important to BCS when thinking about remote authentication solutions, that is disability discrimination and social exclusion. This is not generally an area addressed by those that sell solutions because they are after the large target customer base and might not want to have to implement complex exception handling, but it is mandatory for Government and anyone providing a remote authentication solution to general customers (e.g. it is part of the requirements of The Disability Discrimination Acts (1995) and (2005)).

If a solution is to be made available to the general population, especially a solution provided by Government, it must comply with disability discrimination legislation. In other words, the solution should not discriminate against people because they have a special need. For example, one solution proposed to replace passwords was to use lots of coloured dots on the computer screen and have the person click on a particular sequence of colours. This sounds fine until those that are colour blind are taken into account. Other methods use graphical images in place of passwords, but these require the interface to support detailed graphics and require the person to have good eyesight.

With any IT-related solution, the hardest group to cater for are the blind, but every effort needs to be made to include all groups with special needs. Therefore any solution should have an alternative that is audio-based or Braille-based at a minimum.

There are many aspects to dealing with assured online identity from legal compliance, the technology constraints, ease of use and the ever increasing threat from crime and big business. The IAWG will continue to stay involved as this market develops and new methods are tried to solve the various aspects detailed above.
The IAWG presented at a number of conferences during 2012. In summary these were:

- UK Internet Governance Forum, March 2012 – Workshop;
- Infosec Europe, May 2012 – Workshop;
- EEMA Conference, June 2012 – Presentation;
- Parliament and Internet Conference (PICFOR), 2012 – Presentation;
- UN Internet Governance Forum, November 2012 – Workshop.

These appearances were made as interactive as possible to elicit feedback on the questions raised from UK, European and international perspectives. The questions asked in 2012, covered in the main text, resulted in some interesting viewpoints and feedback, which are detailed in the reports.

The BCS IAWG will continue to progress this work in 2013. The aim is to run a workshop at Infosec 2013 and present a workshop at both the UK and UN IGF events in 2013, along with presentations at other conferences and events. The IAWG will begin a dialogue with the Internet and Jurisdiction Project. BCS has also started a dynamic coalition to discuss and progress understanding of identity on the internet on behalf of the membership and this will be reported in BCS publications, such as this one and IT Now and at workshops for BCS members.

The main areas of focus for 2013 will be:

- the interaction between identifiers for individuals, businesses and ‘things’, in legal and commercial models on the internet and their impact on privacy and security;
- commercialisation of the internet and its impact on identity;
- how identity attributes are being used for non-identity applications.

In addition to the dynamic coalition, presentations, workshops and reports to the membership, the BCS IAWG intends to work with academia to run some citizen panels to test ideas and concepts around the use of identity. The aim is to get the non-IT literate views of how they use identity and the impact online identity has on how they use the internet.

Anyone is welcome to participate in the dynamic coalition on identity. To join or get further information please email identity@bcs.org
Lord Erroll discussed the need for proportionality between privacy and security, particularly in the relationship between the citizen and government when services were being delivered to citizen’s digitally. It was agreed that the starting point should be that privacy is good and security is good. Identity assurance schemes of necessity involve some intrusion into personal privacy. An identity governance framework must therefore recognise that different people will, at different times, require a different balance between their individual rights and the rights they cede for the greater good. It must recognise that too little privacy is just as damaging to society and security (by enabling more criminality or chilling the democratic process) as is too much privacy (by hampering law enforcement or enabling abuse of power). It must ensure that the benefits the internet can bring are not stifled by an over-strict control on who can connect.

Louise Bennett examined identity governance issues to illustrate the context dependency of what is considered illegal or unacceptable activity in different societies. One example was anonymity of social network sites. On the one hand, some parents in the UK campaign for an end to anonymity so that their child can be less easily bullied online. On the other hand, activists who belong to protest groups or banned religious groups in countries with repressive regimes argue that anonymity on social network sites is essential. Similarly, there are radically different views on copyright enforcement on the internet. Copyright owners consider free distribution of their material to be theft that will stifle creativity. Those in free information movements argue equally forcefully that this is protection of an outmoded business model and some copy protection infringes their rights to use what they have purchased as they want. Blocking and filtering are common law enforcement responses to censorship of content and its perceived theft. It was agreed that these are blunt instruments that just drive illegal activity elsewhere. In addition, DNS filtering is widely seen by those in developing countries as stigmatising the majority of legitimate users, since, at times anyone using an IP address with certain country domain names could be blocked from financial transactions and therefore prevented from doing business on the internet.

John Bullard discussed the essentials of identity governance for ecommerce with the participants, saying that there should be ‘no entity without identity’. It was agreed that for global ecommerce to flourish it is necessary for individuals and businesses to be able to assert who they are and for that assertion to be trusted by the other party to any transaction. Interoperability in the commercial world goes well beyond
questions of technology interoperability. Indeed technology itself is seldom the problem and there are a number of ‘standards’ bodies (e.g. OASIS, ISO and Kantara) which exist to harmonise and deliver such technical interoperability. The more difficult areas are legal and policy matters that are also essential ingredients for true business interoperability in the underlying eID framework. In ecommerce the law of contract is vital because it is essential for all parties to know at all times where liabilities rest. There is no need for governments to assert identity for commercial transactions. The essential requirement is for contractual relationships to be clear at a scheme level.

In addition to the above specific discussions, the workshop participants emphasised that reputation and identity are closely related and well-publicised scams become associated with certain countries and reduce trust in doing business with all individuals or entities in those countries. It was pointed out that Facebook is now an identifier of first resort on eBay to establish the reputation of the counterparty. The importance of trusted third parties for internet transactions was emphasised. The requirement for individuals to retain control of their own identity attributes was also strongly supported.
Speakers:

Dr Louise Bennett, Chair BCS Security Community of Expertise, BCS

Mr Roger Dean, Executive Director, EEMA

Mr Andy Smith, Member of BCS SCoE, BCS

Mr Peter Wenham, Member of BCS SCoE, BCS

Mr David Williams, Member of BCS SCoE, BCS

Seminar details: Presentation on identity to Infosec: Infosecurity Europe (London, May 2012)

This was a two-hour workshop consisting of presentations, discussions and a questions and answers session.

The panel presented the findings of the last year of work in identity by the Identity Assurance Working Group. This was followed with a question and answer session to elicit input on the conclusions and thoughts that the IAWG have made. The issues that emerged from our work last year provided a number of topics for discussion this year:

- To what extent does identity help fund the internet?
- Are there transactions where identity is not needed?
- How do you register an identity remotely?
- How can you rely on or trust an online identity?
- How much do we care about fraud?
- How does trust vary with context?
- How do you protect the naive from themselves?
- How do you know who is liable and for what?
• In what situations is redress essential?
• Can you withdraw consent?

Identity governance on the internet is a key element to ensure that everyone has access to a safe and secure internet, to encourage social interaction and enable access to content and ecommerce. Identity governance is hard within a single country and jurisdiction with well-developed consumer protection. It is even harder to achieve globally. However, that is no reason not to try. Identity assurance at some level is vital for successful business transactions on the internet.

Why you need online identity

You need a level of certainty about who the other party is over the internet that is appropriate for the transaction. This covers a whole spectrum of problems from certainty that you have logged on to a legitimate supplier’s website before ordering your travel tickets to being certain you are transferring funds with your bank related to your bank account. The key thing is whether the other party is good for the transaction. Can they deliver the goods, can they pay for the goods, and what redress will you have if something goes wrong?

It is also important to distinguish between an individual consumer doing business and an organisation. If you are doing business with an individual, you might need to know who they are and that might require use of personal data, unless you use a trusted third party. If you are doing business with an organisation, you need to know that the business is legitimate and is the one you wish to do business with. You also need to know that the business has internal systems to check that the transaction is carried out by an authorised individual, who can accept the transaction and associated liabilities on behalf of the organisation. However, as the relying party, you do not need to know anything about the individual processing of that transaction per se in the organisation. There is no justification for the relying party insisting on a personal ID for the individual acting on behalf of the organisation.

Almost no one reads the privacy policy when they sign up to do something they want to do on the internet. At best they might be persuaded to consider the subject rather late in the day, maybe by a responsible adult! The reality is that some people mind about the collection of personal data by commercial companies and governments and some do not. However, many people do not realise that personal data is being collected and might be connected to their identity.

Most young people accept that personal information is commercial currency on the internet, and as far as they are concerned, this is fine because it keeps their costs down. However, for many privacy rights activists this is unacceptable.

The key thing is for individuals to remain in control of their identities and to understand the value of their identity and of the attributes that others might associate with it, such as their buying power, what their interests are, where they are, what they like to do in their spare time and who they socialise with.

This aggregation of attributes to identities helps target advertising. It can also personalise searches, find you a partner, or, in the law enforcement context, it can track the workings of a criminal gang, a terrorist cell or a paedophile ring. How we feel about each of these uses of data aggregated and associated with our identities is highly personal and highly contextual. Most important of all it changes over time.

So does everyone need an identity, or the same identity, for everything they do? The answer is unambiguously no. This was the almost unanimous response from everyone BCS spoke to from many countries throughout last year. The ability to retain anonymity, particularly in countries with repressive regimes is vital and there is no need to know the biological identity of someone you are playing an online game with.
Aspects of Identity

There is every reason for people to want to retain anonymity in some situations, and use more than one identity for different types of transaction.

However, identity assured to some level is needed for some transactions. Most importantly it is needed for commercial transactions, for buying and selling things. You need to know the counterparty can and will supply the goods or pay the price.

You might also need identifiers for some things. This is becoming increasingly important as smart homes and cities and online health take off. You want to be certain you are turning on the oven in your own home. You want to monitor the solar panels on your own roof. You want your doctor to access your blood sugar level and automatically increase the flow of your medication, not someone else’s.

So managing your identity online and the identities of things associated with you is becoming a vital skill. How can we manage this effectively on a global scale with billions of people and a trillion things attached to the internet?

Registration of identity online

Remote registration and verification of identity (the ability to link a person to a pre-established identity beyond reasonable doubt) is very difficult, if not impossible. There are a number of problems surrounding remote authentication (the ability to link a person with a persona or business relationship). These relate to the characteristics associated with the reasons for using remote authentication and the different methods that are adopted. The three main issues are:

• initially linking the person to an identity in order to create and register an established identity;

• a lack of trusted infrastructure between the person claiming the identity and the organisation verifying the identity; and

• no supervision of the decision linking the person to the identity where this decision is performed remotely – basically, there is no oversight that the person is the real identity holder.

Currently there is no complete solution available. The main reason appears to be trusted identity documents (passport and driving licence) have no electronic interface. Data protection laws prevent online checking and corroboration of identity claims. There are also residual risks with no practical solution when the relying party is remote to the identity claimant. The main risks are coercion and duress of the identity claimant.

For many years there have been methods of proving entitlement and identity. Decades ago authentication was down to the handwritten signatures and seals or a face-to-face meeting. Later other methods were introduced to meet changing business practices. These included the use of handwritten signatures on posted forms or witnessed signatures on contracts of high value.

In more recent years, many low risk transactions have moved to telephone call centres, where shared secrets, such as mother’s maiden name and date of birth are used to establish the right to access a service by someone whose relationship has been previously established.

Banks have used various methods for remote authentication for many years: via the automated teller machine (ATM) network, using a bank card with a personal identity number (PIN), via the phone using shared secrets for authentication and via post with a handwritten signature.
The key aspect of all these methods is that the relationship has been set up initially by a face-to-face meeting. For the last 5000 years and until the 1990s, all registrations of high value or where assurance in the identity was required were done face-to-face.

Even now most organisations currently use the passport or driving licence to establish a person’s identity. However, neither document has an electronic interface or supporting infrastructure to permit anything other than visual, or machine-assisted, verification (using custom readers) of the documents. This means that until now there has not been a trusted identity document on which to base a solution.

The need for high assurance remote identity verification stems from the changes brought about by cost saving and convenience offered by the internet and other remote communication channels and by the ever increasing risks of identity theft. So how can high assurance be achieved?

Personal information is now everywhere on the internet, everything from social networking websites to professional organisations, conference proceedings to newspaper reports. Even education and CVs are often online and visible to all. Use of this information can help corroborate the existence and use of an identity, but this information can often let an identity thief know enough about an identity to misappropriate it. The biggest challenge with online registration is being sure that the person claiming the identity is the legitimate owner of it. In order to use remote channels, but also deal with the risks of identity theft and misuse, a method is needed that will not only offer the assurance needed to prove entitlement, but also the assurance in the initial identity in order to establish that entitlement in the first place.

So how can this be done and how good is good enough? For many things, such as downloading documents or even buying items, very little personal information is required and registration of identity mainly involves registering a payment method that works, such as a credit card or PayPal account. Even now applications for certain products such as passport or driving licence still require face-to-face interactions even if that is with a third party, such as the Post Office, to perform the corroboration that the claimant matches the identity.

There are many good examples of where even the best checks have gone wrong, from genuine passports being issued to fraudsters, such as to Charles Stopford and John Darwin. Electronic transactions can also be intercepted. Applying for some things online require a lot of personal information to be entered. A keyboard logger on the user’s machine can therefore capture significant amounts of information, which can then be used to steal their identity. People should make sure they have a good up-to-date antivirus and internet security package running on their machine and only use trusted machines when accessing bank accounts or entering personal information.

Questions still remain, however. How do you register an identity remotely and how can you rely on or trust an online identity?

**How do you trust an identity when both parties to a transaction are on the internet?**

There are two parties in a fraud: the fraudster and the fraud subject (i.e. the seller and the buyer). Fraud has been with us since time immemorial. From the alchemists in medieval times to the snake oil sellers in the gold rush days in early modern American history. Today fraud, while still conducted personally, can now be conducted at a distance over communications infrastructure, be it a boiler house selling dubious shares to the so called 419 (Nigerian) scams, essentially social engineering done electronically. But what about online purchases? How do you know the seller is legitimate or, for that matter, that the credit card is real and valid? How can you trust the other party?

For the moment imagine yourself as a peasant in the Middle Ages and a person comes up to you and tells you they are the King of England. How on earth would you know who they are? There are no televisions,
radios or newspapers to tell you they’re coming, and you have no idea what the King looks like. You therefore have to consider context. If the person is richly dressed, is attended by masses of other well-dressed people, possibly with a small army, you would take it at face value that this probably was the King. If you go in to a shop you expect the staff to be from the shop and to sell you what you ask for. Person-to-person presence tends to work well, especially if you frequent the shop.

If you visit a police station and meet a woman in a police uniform, you fully expect them to be a police woman, but if a uniformed officer comes to your door, would you be so sure, do you know what a warrant card looks like? In comparison, on Twitter you generally expect to be tweeting with a persona and emails could be real or persona-identified depending on business or personal context.

The online context is completely different. Some websites, such as Amazon and Tesco, are trusted because of their reputation, but if you want a tap and it is cheaper on a small plumber’s website rather than a large DIY website, how would you be sure it’s a legitimate seller? Would you check the reputation of the website before buying?

People can be very naive and it is sometimes necessary to protect them from themselves, which is something credit card companies are becoming good at. Without naive people the snake oil salesman would not have made a living, and the same goes in the internet age. ‘you have been selected’ email urging you to click the URL and confirm your prize is a compelling message. What about a tweet from someone you know with a shortened URL link, do you click that? Do you click URLs found in a search without thinking?

It is always worth checking websites’ reputations before dealing with them. It is also worth online companies using secure payment systems, such as those offered by Visa, MasterCard and PayPal.

**Liability and redress**

This is a difficult topic and in many areas there are no clear answers. Hence we wish to engage you in discussions. Let us consider three different scenarios:

- **Inside the UK;**
- **Outside the UK, but inside the EU/EEA;**
- **Outside the EU/EEA.**

The first thing to say is that, particularly when dealing with online situations, you do not necessarily know where your identity information is being held. It might even be in more than one country. You can only be sure of this to a certain extent by reading the small print. Quite often people sign up to having their data transferred outside European DPA protection by agreeing to terms and conditions that permit this.

In the UK, we have a number of laws which have some relevance:

- The Human Rights Act (1998) (HRA);
- The Data Protection Act (1998) (DPA);
The incorporation of Article 8 of the European Convention on Human Rights (ECHR) into UK law via the HRA means a public body engaged in any form of interference with an individual’s privacy must be able to demonstrate that what they do is:

- authorised by law;
- proportionate to the purpose in question;
- necessary; and
- conducted in accordance with one of the legitimate aims set out in Article 8(2) of the ECHR.

It has not been tested fully by law, and proportionality and necessity have not been fully defined and so detailed liability is not assigned.

The use of personal information is regulated by the DPA, which covers the circumstances under which personal information can be processed by public authorities and private organisations. Under the provisions of the DPA, any individual or organisation engaged in the handling of personal information is required to ensure that all information is:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept for longer than is necessary;
- processed in line with rights of data subjects under the Act;
- secure; and
- not transferred to other countries without adequate protection.

However, there are limitations to this and any organisation can ask a user for permission to store and process their personal information in another country, which is often buried in the small print.

One of the key features of the system established by the DPA is that it does not provide individuals with substantive rights that can be enforced by the courts. Instead, an individual who believes that his or her personal information is being improperly held or used must make a complaint to the Information Commissioner’s Office – so no formal liability rests with the organisation holding the data for any form of direct legal action.

The third major piece of legislation we examined was RIPA. Designed to replace the Interception of Communications Act (1985), RIPA established a framework for the use of surveillance and data collection techniques by the police, the security services and other law enforcement agencies. In addition to criminalising the intercepting of a communication over a public network without consent or a warrant authorised by the Secretary of State, the Act set out the circumstances under which public authorities, most notably the police, can engage in various types of surveillance activities. It provided a framework for the authorisation and review of those activities by the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner.
Aspects of Identity

There are proposals to strengthen legislation within the EU by:

- increasing responsibility and accountability – companies would have to notify their clients of any theft or accidental release of personal data;

- clarifying that where someone’s consent is required before a company reuses their personal data, they need to give that consent explicitly – people would also have access to their own private data and be able to transfer it to another service provider more easily.

- reinforcing the ‘right to be forgotten’ – basically the right to withdraw consent, people will be able to have their personal data deleted if a business or other organisation has no legitimate reasons for keeping it.

- applying EU rules when personal data is processed outside Europe – people would be able to involve the national data protection authority in their country, even when their data is processed by a company based outside the EU.

Outside the EU it is difficult to define the legal position on liability.

In practice, in England, contracts are regulated largely by common law:

- Within limits, contracts can create almost any kind of legally binding agreement between parties.

- When things go wrong, most disputes are resolved commercially without recourse to the law.

- These contracts apply just as much in online transactions as offline ones.

- Multiple contracts can apply at the same time.

- But there is room for debate about the enforceability of some terms and conditions (e.g. because some terms might not have been truly agreed or because some clauses could otherwise fail under common law or statute).

- Further, contractual enforceability with regard to children is a matter of some debate.

We have all seen the tick boxes of terms and conditions. Do we read and digest them – I think not. They are often very long, written in legal terminology and tedious to digest, so we do not always know where our identities are held, how the information is used and protected and whether liability flows with the information (and if this liability is protected). Even if we did, it is not always clear how we can take action if something goes wrong. Firstly, how do you find out if things have gone wrong? Then, with a credit card, I suggest you want any errors corrected (including consequential ones resulting from the initial error) and you want financial recompense. This is easy to say, but often difficult to achieve. There is a limited amount of case law and it could be very expensive to create some.

Having consented to someone holding your identity, they are likely to use it and to act upon it. They might well pass part or all of it to others, either in the same organisation or in other organisations. Within an organisation it is very often the case that no-one has overall visibility and takes effective overall responsibility/ownership for the information and for liability if things go wrong. The subject of the identity information should know where it is held, the validity of the information held and what it is being used for – this is often not the case. Withdrawing consent requires goodwill and good practice on all sides together with good communications. Having given someone a piece of information, is it realistic to expect the recipient to forget it?
Once you go outside of EU data protection, all bets are off. In the USA and other American countries it is often the case that personal information is sold. One case from a few years back was of a lady who had a baby in hospital and when she got home she started receiving free samples of baby food and nappies. It turned out the hospital was informing a marketing company of every birth in the maternity ward.

One of the questions that is now being asked is can a person revoke consent and have all of their personal information removed. The view from many seems to be that this would currently be very difficult to achieve because information tends to flow one way and replicate and duplicate on the way. Until there is legislation specifically enabling this right, it is unlikely that it would be possible without significant work by the individual. But is it possible?

**Commercial exploitation of identity**

It is becoming apparent that government-issued credentials are not always effective due to their inability to attract enough applications which can make use of the ready-made registration and authentication process. As we all know critical mass is the success factor required when implementing ICT product and systems. If citizens only use government-issued credentials once or twice a year, then what chance is there of remembering access procedures for other applications.

Admittedly some national identity services are a success (Belgium and Estonia). However, any country in the planning stages should seriously consider a private–public partnership. With these the challenge is convincing the private partners that they can generate money and make a profit from such schemes. In April 2011, the US Department of Commerce released its National Strategy for Trusted Identities in Cyberspace (NSTIC) which called for a public–private partnership to create a secure commercial, social and civic identity ecosystem. The Open Identity Exchange (OIX) has taken the lead in constructing both the rules and tools for the rapid, internet-scale creation of such an ecosystem: the Trust Framework. Other governments have now joined in the call for secure public protocols that protect citizen identities.

On the other hand, most people access their online bank accounts four or five times a month – most with two-factor authentication. If this is acceptable for financial access, then it can readily be used for other commercial applications. It might only be a question of time before two parallel federated identity systems are used for different types of applications: public and private.

In the private sector, the main holders of identity information are telcos, financial institutions (banks, credit cards and credit agencies), social networking sites and supermarkets. Once these start making use of the personal information they have and aggregating the many attributes they have, a critical mass will soon be created.

Interoperability is the key to critical mass. We have seen in the past how this has rapidly usurped the most well-designed and well-planned standards by public use and demand of easy-to-use services.

User online experience is becoming ever more sophisticated with more and more apps becoming available to download, which together with BYOD in enterprise is blurring the identity boundaries with many identities and access protocols on a single device.

Smartphones are becoming the internet-access device of choice for many, especially in developing countries that do not have a fixed phone line infrastructure.

Add in ‘identity as a service’ and the Cloud and you have an almost unmanageable morass of global identities. How can the user manage to keep control of these identities and use them effectively?
Aspects of Identity

We need a trust framework for open identity. At the same time, the negative aspects of online privacy are becoming better understood and more frequently questioned by consumers. These issues are impacting the design and development of consumer identity systems and it’s a question of whether our current offerings, such as SAML with OpenID Connect, can provide the type of identity system that will perform to the expectations of this increasingly sophisticated audience in terms of user control, privacy and security.

Identity as a service raises the question about whether identity and personal attributes are legitimate currency on the internet: can you really pay for things by giving away your personal information and do people realise what their information is worth?

Can the user have any control over aggregation and data mining, or will this growing problem become unmanageable? Even now it is possible to track individuals and find out about their likes and beliefs, which is great for marketing and stalking alike, so what is the risk-reward balance and how can this be better managed?

The discussion raised some interesting questions. It was generally agreed that people do use their personal information as currency on the internet: from giving away email addresses to download documents to giving away personal profiles for things they feel are of value, such as free gifts.

One example of not reading the small print was given. It highlighted the risks. A young lady found a website offering free samples of perfume. The sample was free, but there was a charge of £2.50 for postage and packing, which she duly paid. The free sample arrived, then, three weeks later, a large bottle arrived along with a bill for £89 which had been charged to her card. In the small print it stated that unless the free sample was returned within 14 days and a written request received to cancel the order, a new bottle of perfume would be sent every month for the cost of £89 including postage and packing. This might appear to be a fraud, but it is actually perfectly legal – it is just taking advantage of the fact people do not read the terms and conditions.

Various other examples were given of how fraud had been undertaken through identity misuse or social engineering. The general conclusion was that people should only use websites they trust and should not generally expose their personal information.
Annex 5
EEMA (Paris, June 2012)

Speakers:

Mr Roger Dean, Executive Director, EEMA

Mr Peter Wenham, Member of BCS SCoE, BCS

Mr David Williams, Member BCS SCoE, BCS

Seminar details: Presentation on identity to EEMA Conference in Paris on 13 June 2012

BCS Panel Session – Aspects of Identity

The chairman of this session was Roger Dean and the presenters were Peter Wenham and David Williams. The presentation given was very similar to that given by the IAWG to Infosec in May 2012. The slides will be loaded on the EEMA website and so they are not given here. It was well received, as were copies of the BCS IAWG Aspects of Identity Yearbook 2011–12 which were handed out to participants during the two-day conference. The BCS session was the final one at the end of the conference and so previous speakers had covered some of the issues in different ways. This did not detract from the BCS session. The audience numbered approximately thirty.

There was a question session of 40 minutes at the end of the formal presentation, and because of the questions from the floor we did not use the question material we had prepared but addressed the audience’s issues.

The first questions addressed the advice that users should not open emails if they did not know the sender or were suspicious of its content. We pointed out that computer professionals might do other things such as opening the emails in a sandbox, but that you cannot expect ordinary users to do this. A number of professionals pointed out that they had to sort out malware which their friends had downloaded and opened.

One questioner stated that users should carefully read website policies before entering into a financial transaction. He stated that the world is getting over suspicious of senders of emails. Again it was pointed out that these suspicions were supported by the facts and that policies can also be spoofed. Of those present, only four admitted that they read the terms and conditions before committing a financial transaction on the internet.

A UK questioner said that he felt pressured by the UK Government to talk to them online and to make payments online. His point was that there was no commercial or business model for this: he either wanted this
Aspects of Identity

to be developed or the pressure to do things online removed. It was also pointed out that some countries do not feel inhibited by the lack of models and have pushed ahead regardless.

Questions then focused on fraud. Roger Dean gave figures for online financial fraud in the UK last year in billions of pounds. Another speaker described an issue he had recently with a UK bank where his address had been changed, his Experian record had been altered and money had been withdrawn from his account. The bank wanted eight weeks to investigate and, until they say a crime has been committed the police and the Information Commissioner will not act. Since audit trails show that the account owner had not altered his records he felt that it was an ‘inside job’. Another member of the audience talked of someone using his account (with only partially correct security information) to purchase mobile phones fraudulently. He stated that ‘know your customer’ had not worked in this case. The things that came out of this discussion included:

- the current laws on identity and identity management are not clearly understood and enforced;
- a suggestion that UK laws in this respect need to be revisited;
- that the policeman on the beat knows neither how to handle identity irregularities nor most IT-related crime. (After the meeting we were told that all police in Wales are told whom to pass on all such issues within the police.)

This is an issue that BCS will work on with EURIM as part of their membership of the Digital Policy Alliance. Such matters need to be raised with the UK Parliament and also with European bodies.
Speakers:

The Earl of Erroll, Chair of EURIM

Mr Andy Smith, Member BCS SCoE, BCS

Other panel members

Seminar details: UK Parliament Annual Internet Conference run by PICTFOR

Lord Erroll chaired a panel at the conference on which various aspects of identity were discussed. In the panel session questions were raised by the audience and the panel provided answers. In general there was agreement that identity is a critical issue with the UK Governments ‘Digital by Default’ agenda and needs to be dealt with seriously.

Both Lord Erroll and Andy Smith answered a number of questions related to identity. This lead to a lively debate about the use of anonymity and the accurate use of personal attributes on the internet when trying to protect one’s privacy.

There were various discussions about how to protect oneself online and to prevent identity theft. Issues such as how to protect the naive from themselves were discussed. It was made clear that assured, accurate identity is required for use by Government and some other services, but that commercial services are often happy with a persona as long as that links back to a commercially sound relationship, such as a credit card or other form of payment. However, many websites ask for much more information than they require to offer services and often use this for targeted marketing or to sell a commodity. A suggestion was put forward that people should only enter accurate personal information on websites that they trust, however a debate then took place on how anonymity can be used for things such as cyberbullying. Some of the methods used for protecting privacy and preventing identity being used for targeted marketing and identity theft, such as using inaccurate personal information or different personification, can also be used to create anonymity for nefarious activity.

The balance between privacy and anonymity is an area that BCS will continue investigating during 2013 because it appears that proportionality is not only needed between privacy and security, but also between anonymity and security, in which privacy plays a part. The conclusion was that a lot more work and debate is needed in this area.
Annex 7
UN Internet Governance Forum (Baku, November 2012)

Speakers:

Dr Louise Bennett, Chair BCS Security Forum Of Expertise, BCS

Mr Andy Smith, Member of BCS SCoE, BCS

Mr Ian Fish, Member of BCS SCoE, BCS

Mr Asrar Baig, IT Matrix, Saudi Arabia

Mr John Bullard, IdenTrust

Seminar Details: Workshop on the Aspects of Identity at the UN IGF in Baku, November 2012

Background

Members of the BCS Identity Assurance Working Group (IAWG), supported by IT Matrix from Saudi Arabia and IdenTrust from London, attended the UN IGF meeting in Baku in November 2012 to take forward one of the five calls for action agreed by the Policy and Public Affairs Board (PPAB) for BCS to pursue in 2011–12.

The panel was chaired by Louise Bennett (Chair BCS SCoE) and the other members were Andy Smith (BCS SCoE), Asrar Baig (IT Matrix) and John Bullard (IdenTrust). Remote moderation was performed by Ian Fish (BCS SCoE).

The IAWG prepared a workshop on ‘Aspects of Identity’ for IGF 2012, following up on IGF 2011 and other workshops, including Infosec 2011 and 2012, EuroDIG 2011 and UK IGF 2012. The outcome of these events was reported back at a joint BCS/EEMA Thought Leadership Seminar on ‘eID Enabling Business Transaction’ on 27 November at BCS.

Overview

The meeting in Baku was the seventh IGF. The emphasis and themes are changed each year. This is the second IGF at which BCS have run a workshop. This year the BCS workshop fed in to the plenary session on security, openness and privacy.

The IGF is described as a multi-stakeholder discussion. To date it has achieved consensus on a number of issues, such as ways of dealing with child abuse on the internet (where there is a large degree of
international consensus). The attendees were: parliamentarians, government officials, internet registrars (such as Nominet), business (largely the majors such as Microsoft, Google, Cisco, Nokia) and some smaller businesses and civil society (largely human rights, privacy and freedom of the internet (or, more accurately, free internet) activists. There were also those campaigning for freedom of use of the internet across borders and in various forms of repressive regimes.

The BCS workshop in Baku was designed to contribute to the following questions from the security, openness and privacy theme. The IGF questions that BCS concentrated on addressing were:

- **Question 1** – What impact can security and governance issues have on the internet and human rights (in this case the right to privacy)?

- **Question 3** – What risks can internet fragmentation pose to security, privacy and openness? If identity governance becomes fragmented and requirements change, what impact does this have?

- **Question 5** – What risks do law enforcement, information suppression and surveillance have on security, privacy and openness? Identity information can be used as a tool by state and law enforcement both for good and bad reasons, how do you strike a balance?

- **Question 6** – What measures can be taken to ensure freedom of expression, access to knowledge and privacy, including for children? Can anonymity really be possible on the internet and does this have implications on providing a tool for criminal and terrorist organisations?

There were three main objectives for this workshop:

- To look at the governance of identity on the internet and its impacts on security and privacy.

- To look at the use of identity in commercialisation of the internet with particular regard to legal frameworks and economic development.

- To look at the balance between privacy and openness, in the context of user norms and behaviour, including how to protect the naive from themselves, and how to enable better use of identity for access to information resources and online services.

**Feedback from Workshop 50, Aspects of Identity**

This workshop provided some surprising answers and changes in direction.

The fundamental finding from the BCS workshop at IGF 2011 was that proportionality between security and privacy is culturally and context sensitive, but also very hard to define and a very emotive subject. It is unlikely that there is one balance and there will always be polarised views over the balance between security and privacy. However, the surprise outcome from our workshop at IGF 2012 was that the balance is not necessarily between security and privacy, but between security and anonymity, with privacy being an aspect of security.

The key questions we posed for discussion were:

- Is identity legitimate currency to fund the internet?

- How context sensitive is identity?
Aspects of Identity

- How do you protect the naive from themselves?
- Will we ever be able to balance the need for security with the right to privacy?
- How can an internet identity framework become an ebusiness enabler for the masses in the East?

Session notes

The following are the notes and findings from the panel session.

Louise Bennett introduced the session and the panel, explaining that there would be five-minute presentations from the panel members, each outlining three key issues. The first of these would be commercialisation of the internet with Louise covering the Western view and Asrar Baig the Eastern view of this topic. Governance on the internet would be covered by John Bullard. Then Andy Smith would cover the implications on identity of balancing security and privacy.

The panel discussion was then about an hour and was a good interactive session. Louise explained that the panel was organised by BCS, which is the Chartered Institute for IT in the UK. The Identity Assurance Working Group within BCS has the aim to drive improvements that are needed globally on this subject through the UN Internet Governance Forum.

One topic considered was how to develop valued incentive models that match the requirements of people for identity for ecommerce. The panel looked at the whole framework for identity governance on the internet and the complex topic of trust in transactions with remote identities. This included the use of anonymity, pseudonymity and attribution.

The most fundamental finding from the work last year was the confirmation that security, privacy and anonymity is culturally and contextually a sensitive topic. It’s hard to define and agree, and is very emotive. Proportionality will be raised in every discussion on identity on the internet.

This year, the panel focused on a modified set of issues. The commercialisation of the internet including legal frameworks, the effect on economic development of the internet, the contextual nature of identity and the different drivers for security and privacy and how they can be better balanced.

You need different levels of certainty over the internet about whom the other party is that you’re communicating with and you need a level of certainty that’s appropriate to the transaction that you are doing. This covers a whole spectrum of problems. From the certainty that you’ve logged onto a legitimate supplier website, to being certain that you’re transferring funds to your bank account. That’s a different level of trust for each different type of transaction.

The key thing in every transaction, on the internet, is determining whether the other party is good for the transaction? It’s exactly the same issue as if you were doing it in the physical world. Can they deliver the goods? Can they pay for the goods? And most importantly, bringing in the legal issue, what’s the redress you’re going to get if this transaction doesn’t work and something goes wrong?

If you’re doing business with an organisation, you need to know that the business is legitimate and has processes in place that mean the individuals from that organisation have the authority to undertake the transaction.

You don’t actually need to know the individual’s identity in the organisation. You need to know that the organisation is the right one and has internal systems that are going to check the transaction that’s carried out.
There are a lot of different commercial models on the internet and some services are free or below cost because there is value in the data that we, as individuals and customers, might give up when we’re using those sites or services. Also, we should know that there’s a quid pro quo which is usually targeted advertising. A quote from Blue Beetle was, ‘If you’re using a free service, you’re not a customer, you’re a product’.

There are costs associated with the internet. If you don’t want to pay for those services and access with cash, then you have to realise that maybe you’re paying through your taxes, or maybe you’re paying for it through the abrogation of your activities as an individual identity on the internet. When you talk to young people, they mostly accept this paradigm.

It can be a win–win situation. The individual can get subsidised or free services, access to information, by giving up personal information about themselves and their identity that they think is of equivalent value or less value than the services they’re getting.

If you don’t want your identity attributes to be used and privacy really matters to you, then you either get offline or pay for your protection or pay to understand how to protect yourself. We need to make our own informed choices and these will be culturally and contextually, completely different for each of us at any point in time and over time. We’ll change our views on these, perhaps as we grow older.

The ability to retain anonymity, particularly in countries with repressive regimes, in some situations, is absolutely vital. However, identity assured at some level is needed for many transactions. Most importantly, it’s actually needed for commercial transactions when you’re buying or selling things. You need to know the counterparty will supply the goods or pay the price.

You might also need to know identifiers for some things. This is becoming increasingly important because we have smart homes and online health is taking off. If you’re a diabetic and your doctor is monitoring your blood sugar level remotely and automatically increasing the flow of medication, which is already happening in some places, you need to know it’s your medication that’s being changed, not someone else’s.

So, managing your online identity and the identity of ‘things’, or organisations that are associated with you, is becoming a vital life skill for everybody. How can we possibly manage that effectively on a global scale with billions of people and a trillion things attached to the internet?

Turning to the Eastern view, and more specifically the Arab world, there are significant cultural differences when we look at internet governance or the commercialisation of the internet. The West can benefit a lot if it really looks closely and analyses the Eastern aspect. The East’s and the West’s perspectives of internet security and privacy are at different extremes. In the Arab world people are used to being monitored. In the Western world, people want everything to be more open: and it’s already very open.

Over the past few years, the Middle East has come forward in leaps and bounds on the service side. There’s a lot which can be done over the internet today, including transactions with a government, and a lot other services, like telecom services, airline tickets, hotel bookings, have migrated over to the internet.

When you come on the product side, the East has new challenges. In the Middle East, people are more used to buying tangible products, with a touch and feel.

There are other challenges. The East doesn’t have the real logistics infrastructure in place to manage the goods to go from one place to another – many places do not have postal addresses. The East often lacks the legal framework to protect the consumer, so trusting that somebody will ship something and it will be delivered without problem becomes difficult.
Aspects of Identity

In the Arab world, people trust very much on face value: totally opposite to people in the West. When somebody says who he is, it’s often not questioned, they just want to believe it. Asking somebody to give their identity or to cross question is tantamount to offending them.

This trust on face value is not lost when you go onto the internet; it’s more like, ‘because the technology is there, it has to be true’. Anything which is written on the internet, anybody who writes something on the internet, is considered to be valid. This level of naivety on the internet can be problematic.

Privacy is not so private in the Middle East. The people accept being monitored. Why? Because they have this trust in the government – thinking that the government is supposed to provide them security so they’re going to be monitored.

People in the Middle East aren’t looking at the private sector for providing digital identities to do e-commerce, they’re looking at the government and so they make them accountable or responsible for bringing security to identities on the internet.

One question is why privacy advocates won’t go overboard in pushing the Eastern societies to be more aware of their rights. It is very tough for Westerners and privacy advocates to see that this is a different aspect. From an Easterner’s perspective, the number of people getting onto the internet is huge and it’s multiplying many fold every year. So how can this framework enable the masses in the East to gain benefits out of this quickly?

What boundaries of internet identity would advocates of anonymity accept? When we say the word freedom, there is a definition requirement. What is freedom? And the definition requirement can only be fulfilled if we know the boundaries.

From a commercial perspective, whatever is said about the Eastern view or the Western view, the internet makes no difference at all. Whether you are trading in Birmingham UK, Birmingham Alabama, Bahrain, Bali or Baku, it makes no difference. We have to build some form of framework, some form of trusted identity processes into the picture to enable this to happen.

How do we enable small businesses to interact with their counterparts in a trusted manner so that commerce can take place? The internet offers an enormous opportunity to do this, but we must bring some form of governance, some form of trusted identity processes into the picture to enable this to happen.

What do we mean by trusted identity? We might mean having absolute certainty of who you’re interacting with. We need to know who guarantees the identity of the individual person or organisation? We need to have a complete and transparent audit trail of who did what and when?

We need to see trusted electronic identities as a key component in limiting liability and external exposure, so there must be some form of liability management if things go wrong – where can I look for redress? Those are the key issues we should seek to address from a commercial and from a business perspective around the world.

Identity is a critical piece of a trust model that needs to accompany the commercialisation of the internet. The other two things we need to think about in this context are what aspects of identity are to be managed and who will be covered by any identity management solution.

The technology is the easy bit. It will do what we tell it to do. The human bits become much more complicated, particularly when you look at the liability and legal issues. How can we link together the buyer in Bali and the seller in Birmingham so everyone knows what their liabilities are and are not?
It’s easy to have identity management internally or within a community of interest or within multiple communities of interest, but once you get to multiple communities of interest across multiple legal jurisdictions, it can get much more complicated.

We could have the equivalent of a scheme such as Visa or MasterCard, but in today’s internet era we need to think of the joining up of payments with all other pieces of a transaction, so you need some scheme, some method, some legal liability framework that all parties can sign up to. It is likely that a number of private sector initiatives will interact based upon the law of contract so that everybody knows what their liabilities are and what they are not.

From a government perspective, we would suggest that governments are not in the business of managing their citizens’ liabilities. That is not what government does or should do. Government should make use of these sorts of private sector initiatives in much the same way as governments use the world’s payments networks. They do this today with significant trust.

So one thesis is that, if we can have some form of global contractual structure, through entities like financial institutions, which are regulated at the country level, then it should satisfy all the different blends of government that we have around this planet and instil trust in use of identity.

Security versus privacy and openness is a really contentious issue. It is a very difficult balancing act, and finding the right balance is proving incredibly difficult, if not impossible.

On the one side, you’ve got national security and law enforcement (actually protecting the majority from the minority). This is the government’s obligation of making sure that all the citizens in a country are protected from those who would cause them harm by committing identity theft, fraud, and other malicious activities.

On the other side, you’ve got the right to privacy, you’ve got fundamental human rights, and in Europe, you’ve also got data protection legislation, all aimed at protecting the individual.

In some ways, privacy and the right to privacy is about protecting yourself. Some also claim that anonymity is part of privacy and therefore also a right, so it makes the balancing act even more complicated because some of the things that you’re doing for national security can be misused and used against people. Some of the things you do for privacy can be misused.

More and more, as organised crime moves onto the internet, you’re actually seeing criminals using the laws and rights about data protection and privacy to protect themselves and their activities online, and using those laws to misuse the internet and use it against individuals and against law enforcement.

When it comes to identifying someone how good is good enough? We have a lot of problems with stolen identities. We have a lot of problems with online fraud. Much of that is caused because the root identity cannot be confirmed or cannot be traced or can be too easily stolen or misused. So when you’re interacting with someone, either you don’t know if they are the legitimate person or they don’t know if you’re a legitimate organisation and one they should be doing business with.

From a sort of governmental point of view, if you’re going to give someone a passport, you want to know they are who they claim to be and they are a national of your country and have a right to a passport and a right to travel. However, if you are just letting someone download a free report on the internet, do you really need to see their passport?

We have a lot of people going online, a lot of young people going online. They’re following the crowd, they’re following what their friends do, they’re putting a lot of their personal information on the internet. It’s being captured, it’s being stored, and they can never delete it again.
We have situations where large companies are interviewing people and actually asking to be ‘friends’ with them on Facebook or linked to them on LinkedIn, so that they can see their personal information and the type of person they are and who they consort with. That’s a bad use of someone’s personal information. People might do silly things in their teens and when they go to get a job in their 20s, the people interviewing them can see what they once did and can hold it against them. You cannot stop people from doing stupid things in the first place, but how do you protect the naive from themselves: can you? should you?

Will we ever be able to balance the need for security against the need for privacy? Do we actually need to do it the same for everybody? Can we actually have different forms of balance in different countries, in different jurisdictions and in different contexts?

How do you have any assurance in remote identity? Whether it’s a government dealing with their citizens, whether it’s a commercial organisation dealing with customers, how do you actually have assurance in the identity? Organisations like eBay seem to have got a model to work. They’re using ratings based on feedback. As you interact with them and with other people, your identity becomes corroborated and the level of trust improves. It’s not perfect, but it works. You’re basically getting an identity rating analogous to the financial industry’s credit ratings that are used as measures of trust. Is the concept of online identity ratings one that we want to use?

Currently there are only a few documents for verifying identity. When you apply for a credit card or a bank account, you will usually be asked for documents like your passport or your birth certificate to initiate that new identity you’re creating in that context. But it always comes back to a few documents.

One of the workshop participants raised a very crucial point during the discussion. ‘I think there are a number of confusions. I don’t think anonymity is the same as privacy. People can know who I am without knowing everything about me. I think it’s important to retain these distinctions. And also, at this conference, a lot of people are talking about what their rights are in different places. Quite honestly, I don’t see how you can have rights without having a rights holder.’

Louise responded, ‘I agree with you that anonymity and privacy aren’t the same thing. I think they’re often allied together and this causes an enormous amount of confusion…’

Asar made the follow-up comment, ‘It looks like it’s really a security issue rather than anonymity issue, because the person who will declare something doesn’t like somebody to know it, just because they feel threatened by them. But in an ideal world, if there is ideal security, then we really don’t look for anonymity at that point. Because we have those threats, that’s the only reason we require the anonymity.’

Andy followed up with, ‘I agree completely that privacy and anonymity are different. The biggest issue I have with anonymity is where people actually abuse it and use it to their own advantage, for nefarious means.

Privacy is about not giving personal details to people who have no need to have them. You might give your name, you might give a pseudonym, you might use some form of identity tag on the internet, but it should be traceable back to a root identity in most instances, and it should only be people like law enforcement or intelligence agencies that should be able to do that.’

A workshop participant then made the following point. ‘This problem is often posed as one of drawing the balance between privacy and security. One of my counterparts said we have to optimise for security and privacy. I think that’s even more challenging than just simply drawing the balance between the two, but something we need to try and step up to.

When it comes to the anonymity versus privacy versus security debate, again, it’s an emotive topic, but my view is that this is often characterised as the “if you’ve got nothing to hide, you’ve got nothing to fear” argument.
My problem with that is there are always bad actors in the system, even among those, for example, who have authorised access to data. And under those circumstances, the question is, who do you have something to fear from? Because it might not be the people asking for your information, it might be third parties who don’t have your best interest at heart. That’s something that needs to be designed into these kinds of systems.’

Louise made the point that reputation and trust are other very important issues and reputation is not only important to individuals, it’s also enormously important to institutions.

We have to trust the market to deliver some of these issues and there’ll be some absolutely trusted organisations that people will be comfortable in going with. If people become sufficiently uncomfortable with a particular policy of a particular organisation or its reputation gets damaged or people lose trust in it, they will simply move to a competitor. Many websites have gone out of business when they have lost customer trust. Those that protect their reputations have become household names.

John made the point, ‘I think the key issue there is liability. If something goes wrong, where do I get recourse from? That seems to me, when all else is said and done, to be incredibly important for trust and for doing business on the internet.’

Asrar provided a slightly different view on this point, ‘I believe there’s still a balance required, because sometimes things like the financial collapse in 2008 and the dot com collapse occur, when everything goes wrong by just leaving it to the market. There is a responsibility and accountability required by somebody.

There has to be somebody on top of the regulators. You are required to have a framework, if you just leave it, the banks can do it the way they want to do. The market is just being driven by money, profit. If you leave it to be driven by profit, who will look after the real interest of customers?’

The panel then moved on to another question posed by a Dutch participant. ‘In real life, you have a right to be forgotten. When you don’t want something you have produced or anything else, in the market anymore, you have the right to ask to take it out of the market. On the internet, it’s not possible. What’s your opinion on that?’

Andy made the point, ‘If you post stuff on the internet, it’s there forever. It will get copied, it will get backed up. You try and delete it from one source, you’ll find it on another source. You have this problem in the real world as well. Once you’re in a printed newspaper or on TV, you will never be forgotten, you just have to be careful in the first place.

Around London there, are over 7,000 CCTV cameras, which are run and monitored by different parts of the Government. On top of that, you’ve got tens of thousands of CCTV cameras put in by industries, business, even private individuals. Nobody sits and watches all of that, all the time. The police have only 12 people looking after their cameras. If something bad happens, they go and find the tapes and they look. That’s pretty much what’s happening with the internet. And with data capture on the internet, nobody’s looking at it, there’s just too much of it, but if something bad happens, they can have a look at the tiny little bit that that’s relevant.’

You have to understand from a proportionality point of view, it’s not that they’re tracking everybody, it’s that there’s loads of big computer systems storing loads of data that could potentially track everybody as and when they need to, they go find the bit that that’s relevant. They don’t have the resources to do it and they also don’t have the inclination to do it either.’

The final discussion point was on how can an internet identity framework become an ebusiness enabler for the masses in the East?
Aspects of Identity

On participant commented that often in the East the main issue is with ebusiness. ‘It’s two things. Getting a credit card is a pain. You have to be already employed, and then it takes a while. And the second issue is that people have a fear of getting their identities stolen by a hacker and all that, because during the late 1990s, there were a huge amount of hackers.’

Asrar made the point that there are companies trying to address this. ‘There’s a start been made by a Canadian company in UAE. This company shifted its business model to the Arab world. They said there are too many blue-collar people working in the Arab world who are not even connected with any kind of internet identity or access to ecommerce or ebanks or so on. They started by putting their own ATMs around different organisations which have got a few thousand employees and issuing cards to every single employee.

Now those staff have started to have an internet identity. The same card can be used anywhere across any of the participating countries because it’s really a debit card, which can be used everywhere. The same organisation, which isn’t a bank, is now acting like a bank by starting to give micro-financing. People can take out small loans. All of their money transfers can be done using the same card. So it suddenly gave them a lot of ease.’

BCS have made a lot of progress in the last two years, defining what the problem is and coming up with answers, but the balancing act between security and privacy and openness is going to remain emotive and it’s going to remain very hard. We’re just going to have to work hard on this and the UN and UN IGF are very good forums to keep this moving forward.

Conclusions

The balance might not be between security and privacy. Both of these are about protecting people and protecting people’s rights. The balance is more between security and anonymity. Privacy is difficult to misuse, anonymity can and is misused. Even though anonymity intrinsically provides privacy, there is a significant difference between privacy and anonymity.

Anonymity is the ability to perform actions without them being traced to the person. This means that they have the right to free speech without fear of repercussions, but also that people cannot be held accountable for their actions.

Privacy is the ability only to provide personal information to those entitled to it by law or that the person chooses to provide the information of their own free will.

Privacy protects people’s rights, but does not damage the need for national security and law enforcement, which is normally built in to privacy and data protection laws. However, anonymity can. Anonymity is not necessary for privacy, but is often misinterpreted as a requirement of privacy. Anonymity is not necessary for privacy and the two concepts should be separated.

Anonymity is only required where free speech or other actions could have negative repercussions against the person. Free speech is a legal right in most Western countries, and anonymity can be used to avoid charges of libel and slander or for nefarious actions including cyberbullying.

Therefore the issue is not security versus privacy. They both have the same goal of protecting people. The balance is between security and anonymity.

It is vital to have the right level of identity assurance for the context of a transaction over the internet. The assurance in the identity is context sensitive and can change from anonymously downloading pages from a news service to very high assurance when transferring funds between bank accounts.
In all cases the identity needs to be registered to the level of assurance required for the transactions, which means there needs to be effective methods for remotely identifying someone and issuing credentials.

Basing identity on a liability model and using a contractual framework would significantly improve the trust and commercial use of identity on the internet. Having some method of holding people accountable for their actions and for use of a trusted identity would significantly improve both national and global online commerce.

However, for identity to stand up in court and be viable under a contractual framework, high assurance identity, meeting the tests (using a UK example) of ‘balance of probability’ for civil prosecution or ‘beyond reasonable doubt’ for criminal prosecution would be required.

Identity is used as a form of currency on the internet, with people providing personal information in order to gain free or low cost services in return. This allows the ‘payment’ of those services to come from targeted marketing and other sources. However this does expose people to risks they might not realise. Data mining of the same aggregated data sets can be used for both targeted marketing and targeted crime.

There is still a lot of work to do with balancing and understanding the different drivers for security, privacy and anonymity, including how they pull against each other or overlap. This will be the theme for work next year.

Digital identity is an ongoing piece of work and becoming a critical subject for the success and globalisation of the internet. The key is going to be to define a governance structure that will actually work and the conclusion was that IGF can play an important part in providing the stage for discussions. Such discussions are needed between the IGF meetings, therefore a dynamic coalition is needed and BCS has set one up for identity. Anyone is welcome to join and can do so by sending an email to identity@bcs.org with their contact details.

Most digital identity is still fundamentally based on physical identity issued by a single authoritative source (normally government). The original documents tend to be the national passport or other government identity documents such as ID cards or driving licence. This might be used directly to set up a digital identity, or indirectly, where it is first used to get a bank account or credit card, which is then in turn used to get a digital identity. There are currently no effective methods of creating only a digital identity. Every digital citizen is still a citizen of somewhere.

People need real incentives to get online and perform commercial activities, such as the card for blue collar workers originally started in GCC, but now moving in to Saudi Arabia. Here a real-world (physical) card can act as a digital identity and allow holders to go online and perform commercial transactions. But again this card is provided under a commercial framework and contractual model.

People also need to be helped to secure their online profile so that they are not subject to identity theft and fraud. Weak identities that have been exploited for criminal acts and a few media stories are already resulting in fear of going online across much of the Middle East. Schemes like the GCC card will help to rectify this, but user education and in some places, media education is also required.

Fear of going online and being subject to identity theft is also prevalent in the West and much still needs to be done to help people to understand how to protect their identity and their privacy.

We should not be looking for a grand scheme, but rather small steps and maybe compatible standards so that small schemes can interoperate effectively. However, someone needs to set the standards and this is another task that the IGF, along with standards making bodies such as IETF and ISO, could achieve.
Annex 8

BCS EEMA: Thought Leadership seminar on eID enabling business growth – one year on

Speakers:

Dr Louise Bennett, Chair BCS Security Forum Of Expertise, BCS

Mr David Rennie, Cabinet Office

Mr Roger Dean, Executive Director, EEMA

Mr Adam Thilthorpe, Executive Director, Policy and Public Affairs, BCS

Mr Chris Ferguson, Programme Director, Cabinet Office

Seminar details: To summarise the work BCS has done on identity over the last year for the benefit of BCS membership and EEMA members.

Opening session

David Rennie of the Cabinet Office introduced the day. ‘This is a very timely conference due to announcements released today. We will learn of the differences between the public and private sectors, and look at solutions and where collaboration and competition cross.’

Adam Thilthorpe introduced BCS, its objectives and activities. Roger Dean then introduced EEMA, its objectives and activities.

Keynote (Chris Ferguson) – UK Government initiatives to engage with industry and Europe

The Cabinet Office went for a federated identity approach. In April 2011, it issued a mandate to set up an online services model for government and industry. The issues to be considered were simple authentication, but more robust than social media credentials balanced with the right to be recognised in a digital world.

To assert their identity in a robust and trusted way, which will realise enormous economic benefits, with the ability to have user needs focus first and government requirements second.

Trust is a two-way street. The trust model is a hugely important subject creating a trustworthy digital ecosystem. The Cabinet Office recently announced the creation of the digital identity scheme enabling a cross-government framework for a digital recognition service; however, it’s easier said than done: by putting the power back into the hands of the user and making the back office solution easier.
Annex 8 BCS EEMA: Thought Leadership seminar on eID enabling business growth – one year on

The Cabinet Office is governed by an advisory group which has drafted a policy document; this has generated several cross-government issues. Other partners include HRMC and DWP and alpha projects such as the British Retail Association and the lasting power of attorney, which currently is an all paper process.

All this should provide benefits to the private sector, in terms of fraud protection, regulatory compliance and financial inclusion.

Panel session: Public sector focus – issues and challenges for a cross-government framework on digital assurance

• **Steve Dover, Corporate Director, Universal Credit Programme Business & IT Solutions, DWP** – Designed to overcome the challenges for the citizen and signed up by seven identity providers to the framework, which is still a fledgling and fragile market. We have to be careful with the message which is portrayed to reach a common interest and goal. We have to create a vision and bring it into reality to work for the citizen and DWP. We have to ensure that the foundations which we have laid down have produced a realistic and workable solution.

• **Brigid McBride, Programme Director, HMRC** – HMRC has 39 million PAYE customers. The main issue with citizens is that their contact with HMRC is maybe only once a year, so we must make it an easy and simple process. We have 9 million business (SME) customers and 4.5 million corporate customers. Our challenge is how to fit an IDA solution in front of these systems and models. In addition 10.5 million customers are registered on the Government gateway and these will have to be migrated onto the new service.

• **Tim Wright, CIO, Department for Education** – Where does education fit? We are dealing with children and we have a very disparate network (400,000 individuals). The challenge is to be able to gain access to this information in a secure and controlled way. We created an employee authentication service in 2010 as an EAS shared service. We then created a registration body and issued them with a recognised credential. A federated service followed through the local authorities to build the trust with private service providers.

• **Jim Purves, Head of Identity Solutions, Experian** – Experian provide trust services to many types of organisations. We have to move to embrace these new services in a consumer centric way. We can manage the risk via various online checks that do not require any user responses, such as a consistent IP address and perhaps the position of their phone. We have to innovate to sell these services to other organisations. Trusted parties are allowed to check credentials online. The challenge is how do you manage fraud across these new services and how do you provide uniqueness in a European context?

• **Toby Stevens, Identity Assurance, Post Office** – The Post office completes 11.5 million ID checks every year, it is therefore logical to become an ID provider. The risk is providing a brand new commercial model where the PO gets its revenue from results in a per transaction or registration model, and paying to receive validation attributes. The challenge is being able to work in an agile environment and commit the funding from the start. Many organisations are not committing until this model is proven to be commercially viable.

Questions

**To what extent do you see the opportunity of new service providers being a benefit or distraction?**

SD – The ID marketplace needs nurturing and help during the initial stages, major Government departments need to play their part with integrity to grow this and get it on a firm footing.
BMc – When you build up the stack of Government systems and bring together sustainable solutions, this is the start of the journey.

JP – We need technical interoperability and mutual cooperation or we will miss the opportunity, branding of the scheme and the right message are essential – it has to extend from central to local government services. Finance industry will not get involved until there is a proven business case.

TW – It is essential to have trust, manage risk (cultural issues) and adhere to process standards in a cost-effective way.

**In terms of identity assurance, are the identity providers managing risk in a secure way?**

TS – One method to safeguard this is to reuse existing data for authentication to a relying party – this will evolve into a citizen centric environment with consent for each transaction. It is up to ID providers to provide a user-friendly client.

**The trust and privacy challenges are big issues that must be considered, you can’t retrofit security into these services, can we be assured these have been considered?**

SD – Trust, confidence, privacy and security are top priorities, ten major security segments were considered for Universal Credit; concern centres around those customers who can’t and those who won’t – how to address these and convert them into those who can, there are families who have not worked for seven generations – it’s a culture attitude.

JP – Consumers care about convenience first followed by privacy and security, we need to have these discussions with the IDP programme to drive down the cost of these services, but the size of the market will be much greater.

**Results and recommendations from the BCS eID workshops**

Louise Bennett, chair of BCS Identity and Assurance Working Group

The BCS IAWG found during 2012 that the debate on identity governance on the internet had moved on and become both more realistic and more nuanced.

Five issues emerged from the workshops:

- Tension between security and anonymity;
- Tension between big data aggregation and privacy;
- When do you need a chain of trust and when a network of attributes?
- The value of aggregation and data mining; and
- Liability models –
  - When do you need a trusted identity?
  - When are attribute identities good enough?
Digital identity is becoming a critical subject for the success and globalisation of the internet. The key is to define a governance framework that is pragmatic. There is a need to improve the management of governance on the internet and identity usage so that, in general, privacy is upheld, but where necessary someone can be held accountable for their actions. With more devices becoming networked and people becoming more comfortable using digital channels, the need for reliable means of securing and protecting the identity credentials of individuals is increasing. It is vital to have the right level of identity assurance for the context of a transaction over the internet. Basing identity on a liability model and using a contractual framework would significantly improve the trust in both national and global online commerce. There also needs to be a debate on when authoritative government approved identity credentials (such as those based on passports) provide the appropriate identity model and when an authorisation model based on the attributes associated with multiple low assurance sources (such as those used to gauge an individual’s reputation in online auctions) are appropriate.

Identity is a key issue and facility in the public and private sectors and there are many opposing views which must be resolved. There is no ‘right’ answer. We must continue to have a dialogue to ensure commercial identity transactions across the internet are trustworthy and take account of the different cultural views of security, privacy and anonymity. Tension exists between security and anonymity and big data aggregation and privacy.

Privacy protects people’s rights as opposed to national security and discovery through data aggregation (i.e. where is my personal information?) There is a vast network of your attributes which people are willing to trade for other products and services, if you don’t want to have your attributes available you have to get offline. Identity data is an internet currency.

In business, liability is a big issue and we have to use an underlying trust model to ensure this is effectively managed, such as in a banking model. You have to decide if the ID is real or rogue? How do you get redress? Are all identities the same? Managing your identity online is becoming an essential skill.

The Middle Eastern view of internet commerce is ‘privacy is not so private’ with a real fear of identity theft and fraud.

We should not be looking for a grand scheme, but rather small steps and globally compatible interoperability standards, so that schemes can interoperate effectively. We also need to help people understand the levels of identity assurance they need for different transactions to remain safe online and minimise the risks of identity theft. There is no silver bullet and BCS aim to develop practical governance and management can only be achieved in small steps.

**Panel session: Current privacy and esignature perspectives**

Welcome by afternoon Chair, Neil McEvoy, Managing Director, Consult Hyperion

- Data is to the information age as oil was to the industrial age.

- **Hans Graux, Partner, time.lex, Belgium (EU Directives and Regulations)**
  - There are two legislative proposals – they are both regulations so are binding in law on member states and will replace local laws.
Aspects of Identity

- eID and Trust services regulate that each member state has to accept the ID credentials of other member states who have been notified of their ID credentials.

- Data protection – more extensive than previous laws and will mean major changes to some member states, including privacy impact risk assessments.

- The new regulations are much more strict, complex and explicit, concerned with the protection of minors (i.e. there are no people under the age of 13 on Facebook). The right to be forgotten is almost impossible.

- Timelines are for this to go through parliament and become law by end of 2013–14.

**Stephen Mason, Barrister and Independent Director, T-Scheme (UK situation)**

- You can’t rely on just the IP address for ID authentication, there is no certainty that an eID signature provides absolute proof that it comes from a particular person. Everyone uses electronic signatures in one shape or another.

- T-Scheme manages a certain amount of checks which might be unrealistic and uneconomical for private IDPs or CAs. Forty per cent of children are aware of the privacy issues and use several pseudonyms.

- Belgium fraud lawyers have issued a summons to Yahoo! to supply emails and Yahoo! have replied, ‘We are based in the USA and do not abide by European law.’

**Lizzie Coles-Kemp, Royal Holloway (RH), University of London (Citizen Centric Privacy)**

- Privacy issues – how will the citizen engage with Government services? A project has started to look at online privacy with groups who do not usually engage with Government services. RH focused in deprived communities in the North East of the UK – surveys and focus groups didn’t work, so they used theatre to engage with communities using collective narratives (i.e. clowns were very successful); they encountered engagement, refusal, resistance and exclusion, and family sharing of knowledge, there was a real value in social networks to draw in participation.

- Social networking is a very important lifeline for under-13s; do the youth of today have different attitude to privacy compared with most adults?

Panel session: Private sector focus – Commercial opportunities, federated identity, partnerships

**Nicky Hickman, representing Verizon** – What is the real value for employees or citizens? There must be a clear separation between social data and private data. Identity and personal data provide advantages, you can save money and get more benefits, save time, establish trusted relationships, access to more good quality services. The way to make money from identity is to reach to lots of people.

**Don Thibeau, Chair of The Open Identity Exchange (OIX)** – OIX is a team of rival companies and sectors who compete with each other in terms of who will control the identity. Why do companies join the OIX? Fear and greed – if you want to sell more online you must overcome these issues. Amazon, Facebook and Google are a success because they have overcome the identity issues. European countries as a whole trust their governments more than the UK or USA who have decided not to issue government-backed identities. Interoperability issues are at the rules (policy) and tools (technical) levels.
• **Alex Scandurra, Director Information Strategy and Business Development, Barclays** – Who are our customers? We rely too much on a paper-based system. We find when speaking to customers there is a huge distinction between consumer goods and internet commerce, the roll of the trust network must be scalable between the owners, the issuers and the requesters. We need to build trust, otherwise opportunities will be missed. We are moving much more towards behaviour as a means to identify people.

• **Richard Braham, Distance Selling and Consumer Credit, British Retail Consortium** – IDA shows clear commercial benefits that you can sell more things in a simple and integrated way, but how do we build the bridges? Which is why we are involved with the Cabinet Office alpha project. UK ecommerce is one of the world leaders, however, liability is a big issue. Risk and data is a compromise, a consumer choice, if they want points they give up some rights.

• **Paul Downhill, Consumer Affairs Manager, Home Retail Group** – Online age validation – only assert their age attribute and not their whole identity credentials, failure to comply is a criminal offence. Checking age for purchasing knives, DVDs, alcohol and spray cans – Argos, Homebase. Retailers want age validation included in transaction, it has to be seamless, accurate and free.
BCS, The Chartered Institute for IT

The Institute promotes wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 70,000 members including practitioners, businesses, academics and students, in the UK and internationally.

We deliver a range of professional development tools for practitioners and employees. A leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.

www.bcs.org

BCS Identity Assurance Working Group

In 2011, BCS, The Chartered Institute for IT, consulted its 70,000 professional members worldwide to determine what they considered to be the most important IT-related issues facing governments in delivering savings, stimulating innovation and enabling ecommerce. One of the key issues was to ensure individuals, not organisations, remain in control of personal information and that individuals should control their identity authentication, which is essential for ecommerce and egovernment to thrive.

Over the last two years, the Identity Assurance Working Group has been examining governance and other issues surrounding identity assurance on the internet. In 2012-13, the group continued the thread of the work reported in the 2011-12 Yearbook through a second series of workshops at UK, European and UN events. The results build on the group’s previous findings, continuing to explore the drivers for and proportionality between security, privacy and anonymity on the internet. It also explores practical issues associated with commercialisation of the internet including: improving trust through transparent liability models and contractual frameworks; the value of identity attributes as currency on the internet and other incentives to go online; identity discovery through data attribution; identity theft and fraud. The group once again conclude that there is no possibility of a globally acceptable ‘grand scheme’ for identity governance, but shared sovereignty, based on no trans-boundary harm is a feasible way forward.