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 e-commerce. 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 e-commerce and e-government to thrive. The Identity Assurance Working Group was therefore established to examine the governance and other issues surrounding identity assurance on the internet.

The group ran a series of workshops at UK, European and UN events to collect national and international views and explore the key underpinnings of identity assurance principles, rights and responsibilities, including information rights and privacy, in an interactive and multi-stakeholder format. The collective results are presented here, together with the critical issues on which the group will focus its continued dialogue throughout 2012.
Aspects of Identity

Yearbook 2011–2012
Supporting statements

The BCS Identity Assurance Working Group is to be congratulated on producing this much needed and definitive paper on Aspects of Identity. It seems to cover every aspect of a problem that is increasing in ratio with the explosion of communications in our modern world, on top of which there is strong Government encouragement to go ‘digital’. (I have spent quite a proportion of this morning registering online for VAT for the first time – an interesting experience; I now have a 12-digit ID number!).

This paper is going to stimulate many like me, who have their own views on many aspects of the subject, perhaps no single silver bullet, but at least no longer will solutions be looking for a problem, here it is, loud and clear.

Lord Renwick, President of the Information Society Alliance (EURIM)

Secure and proportionate means of asserting identity are fundamental to the Information Age. It is essential that individuals are empowered to manage their electronic identities and are able to assert just that level of information that any given transaction requires.

Jim Norton, BCS President 2011

The internet is a vital tool for economic growth. For ecommerce to thrive, trusted and interoperable identities are needed for consumers and businesses. We also need clearly articulated, internationally recognised contract liabilities that everyone can understand and enforce. EURIM supports BCS in its drive to get international agreement to a federated model of identity governance on the internet.

The Earl of Erroll, Chair of the Information Society Alliance (EURIM)

BCS, The Chartered Institute for IT, has done a great job in promoting discussion of identity governance on the internet. There cannot be a single, rigidly defined system because people with a variety of different social and cultural backgrounds have very different views about internet governance, but we can’t afford to ignore the issue. We urgently need an internationally accepted model for identities on the internet. I wish them every success in taking this topic forwards.

Rt Hon Alun Michael JP MP
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>vi</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>2 Background on Key Aspects of Identity</td>
<td>3</td>
</tr>
<tr>
<td>Citizens rights and control of personal data</td>
<td>3</td>
</tr>
<tr>
<td>Minimising access and controlling privacy</td>
<td>5</td>
</tr>
<tr>
<td>Registration authorities and ID assurance</td>
<td>7</td>
</tr>
<tr>
<td>Rights and responsibilities of ID providers</td>
<td>10</td>
</tr>
<tr>
<td>Security versus privacy: the balancing act</td>
<td>12</td>
</tr>
<tr>
<td>Identity governance on the internet</td>
<td>13</td>
</tr>
<tr>
<td>Trust in transactions with remote identities: anonymity, pseudo-anonymity and attribution</td>
<td>15</td>
</tr>
<tr>
<td>3 Ways Forward</td>
<td>17</td>
</tr>
<tr>
<td>Identity governance on the internet</td>
<td>17</td>
</tr>
<tr>
<td>ID for ecommerce</td>
<td>19</td>
</tr>
<tr>
<td>ID for egovernment</td>
<td>21</td>
</tr>
<tr>
<td>ID to combat ecrime</td>
<td>22</td>
</tr>
<tr>
<td>Issues of privacy and security</td>
<td>23</td>
</tr>
<tr>
<td>Commercial exploitation of identity</td>
<td>24</td>
</tr>
<tr>
<td>4 Conclusions</td>
<td>26</td>
</tr>
<tr>
<td>Views of the internet reflect societal background</td>
<td>27</td>
</tr>
<tr>
<td>Identity doesn’t just apply to people</td>
<td>27</td>
</tr>
<tr>
<td>Required levels of trust and assurance depend on context</td>
<td>28</td>
</tr>
<tr>
<td>A framework that promotes cross-border trust is needed</td>
<td>28</td>
</tr>
<tr>
<td>5 Recommendations</td>
<td>29</td>
</tr>
<tr>
<td>Annex 1 The IAWG and its activities in 2011 and proposals for 2012</td>
<td>30</td>
</tr>
<tr>
<td>Annex 2 Infosec: Infosecurity Europe (London, April 2011)</td>
<td>32</td>
</tr>
<tr>
<td>Annex 3 EuroDIG: The European Dialogue on Internet Governance (Belgrade, May 2011)</td>
<td>36</td>
</tr>
<tr>
<td>Annex 4 UN IGF: Internet Governance Forum (Nairobi, September 2011)</td>
<td>38</td>
</tr>
<tr>
<td>Annex 5 Parliament and Internet Conference (October 2011)</td>
<td>43</td>
</tr>
<tr>
<td>Annex 6 BCS/EEMA Conference (October 2011)</td>
<td>45</td>
</tr>
</tbody>
</table>
Aspects of Identity – Yearbook 2011–2012 is an important publication for all of us concerned about the issues of identity on the internet. Published by Britain’s influential BCS, The Chartered Institute for IT, it reports on a major initiative by BCS members to understand broadly digital identity issues that were, only a few years ago, considered an esoteric specialty. Given the role of BCS in shaping the education of the whole information technology community, we can expect to see increasingly broader and deeper understanding of identity and privacy by IT practitioners.

The Yearbook is alive and sophisticated. Penned by survivors of a year-long multi-national tutorial on wrong-headed approaches to identity, it wisely challenges us to avoid over-simplifications and unexamined suppositions, guiding us to consider key issues requiring more understanding and consensus.

Importantly, the Yearbook’s authors plant a number of stakes in the ground (for example, around empowering users to control their private identity information) that constrain the scope of argument and will help practitioners arrive at conclusions consistent with our democratic traditions.

The Yearbook represents a moment on a journey rather than a set of conclusions, and that moment is ‘now’: I strongly urge people to read the report and participate in the conversation it animates. Further, since the report consistently situates the problems of identity as being international in character, I recommend this report to audiences around the globe.

On behalf of other readers I offer the authors our thanks and congratulations.

Kim Cameron
Paris, 2012
1 Introduction

Identity assurance is one of the most important issues facing governments wishing to use IT to deliver savings, stimulate innovation and promote efficient ecommerce. Trusted reliable identities linked to electronic credentials are needed to underpin many transactions, particularly where money changes hands or valuable services and entitlements are provided to citizens meeting defined nationality, age or other status tests. The OECD has stated that digital identity management is at the core of the internet economy.¹

Recognising this, BCS established an Identity Assurance Working Group (IAWG) for 2011 to promote understanding of the topic. This report summarises activities undertaken and progress made during the year.

Identity assurance should not be seen as a straightforward problem seeking a technology solution. It is a problem with many socioeconomic risks that must be understood and addressed. These include such factors as: ‘how are individuals empowered to control their private identity information and give informed consent to its use?’ and ‘how are the problems of compromised end-points to be addressed?’

There are intrinsic risks associated with the creation of identity data, maintaining its integrity, security and non-repudiation that demand the highest standards of governance. It is essential that governments lead the way by ensuring identity assurance is trusted both by their citizens and international partners and is fit for a wide range of purposes.

Governments also, specifically, need to: be able to identify their nationals, collect taxes and deliver a wide range of services efficiently without fraud; warrant transactions and contracts within government and with their suppliers nationally and across borders; ensure that the global internet is a safe and trusted place to do business.

BCS supported the conclusions of the 2008 Crosby Report on the challenges and opportunities of identity assurance.² The report put forward a very important principle, namely that:

‘...the citizen should “own” their entry on any [identity] register [when a scheme requires this] in the sense that it should not be possible, other than for the purposes of national security, for any such data (to include digital representations of biometrics) to leave the register without their informed consent. Verification of identity should be performed without the release of data.’

---

This is a principle that BCS endorses and believes must be at the heart of identity assurance schemes. The BCS position is that individuals, not organisations, should remain in control of their personal identification, whether held by governments or other organisations. This means that individuals should control their identity authentication, which is essential for ecommerce and efficient egovernment services to thrive. Privacy is a growing area of concern and needs to be addressed proactively to allow innovation to thrive and public confidence to be maintained in the application of new technology.

Extending these principles to ensure that trust in identities can be established amongst differing cultures and jurisdictions is fraught with difficulty, yet is vital, of course, as the internet transcends national boundaries. At the moment the UN Internet Governance Forum (UN IGF) is focused on internet governance. BCS has set out to influence this through the work reported here, by introducing the concept of ‘identity governance’.

Identity governance is the means by which those who need to rely on internet identities will be able to gain the confidence that they require in accuracy of the identity information that they obtain. It is an emerging concept that BCS IAWG thinks is both important and in urgent need of further work. Neither the centralised, hierarchical model favoured by public key infrastructure (PKI) schemes, nor the less formal models based on reputation or ‘webs of trust’ seem able to scale to global size.

We are not advocating a single UN-run system of global identity governance, but an agreed system for federating many identity governance schemes, with differing levels of trust and security, that all citizens can have confidence in when they need to use such schemes to protect their activities on the internet, irrespective of the jurisdiction they are in. In all considerations about identity assurance it should be noted that honest citizens and criminals will have very different views on rights and responsibilities and for success an appropriate proportionality between law enforcement and individual privacy must be maintained. In addition, the scope of identity data is continually expanding. For example, it now extends to positional data in relation to such things as targeted advertising.

In 2012, BCS plans to continue this work, in the hope of influencing both the UK Government and international institutions (Annex 1).

Disclaimer

A variety of views are summarised in this report. These views do not necessarily represent the position of BCS, the individual members of the IAWG or any of the organisations to which they are affiliated.
2 Background on key aspects of identity

The aspects of identity that the IAWG identified as issues at the start of the year are covered in the first five subsections below. The balance between privacy and security (issue 5) emerged as the most important and contentious issue of these five from Infosec (Annex 2) and the Plenary Session BCS ran at EuroDIG in Belgrade (Annex 3) and together with issues six and seven, discussed at the UN IGF workshop (Annex 4).

1. Citizens rights and control of personal data.
2. Minimising access and controlling privacy.
3. Registration authorities and ID assurance.
4. Rights and responsibilities of ID providers.
7. Trust in transactions with remote identities: anonymity, pseudo-anonymity and attribution.

Citizens rights and control of personal data

The key issue is that in the virtual world each of us may want to know whom we are dealing with, but with varying levels of certainty according to the context of our interactions. In some circumstances (particularly in repressive regimes) anonymity may be the most important thing to us.

When we identify someone, we sometimes want to establish that they are a unique biological being and sometimes that they are the same ‘persona’ who did something at a different time. This has implications for the successful running of a multi-level identity assurance scheme. When do you need to know the biological entity and when do you merely need to know that you are dealing with the same avatar or persona you interacted with yesterday? You need to know a biological identity when you are issuing a passport, but only the persona when you engage with someone in an online game. If a person wants to withdraw money from the account they opened last week, the bank only really needs to know the persona they are using. This is because, in banking transactions, all that matters is that the bank is dealing with the same persona who opened the account and deposited the money (so they are ‘good’ for the transaction). Legislation, such as for anti-money laundering, may mean that the bank is legally required to ‘know their customer’, but the bank does not actually need this to undertake the transaction between the two parties: bank and customer.
So, how can an individual control access to their biographic (and in some cases biometric or positional) data after enrolment in an identity scheme, as put forward as a key principle by Sir James Crosby?

First, some definitions are needed that will be used throughout this report:

A service provider that creates, maintains and manages identity information is an identity provider. A relying party is an organisation that uses identity data as part of its provision of services. The individual to whom an identity and associated identifying data relates is the identity subject.

The identity provider, relying party and identity subject all have both rights and responsibilities with respect to the collection, retention and sharing of identity-related data.

The most onerous responsibilities lie with the identity provider. They must confirm identity to the level required at enrolment, including matching the identity subject to appropriate aspects of their biography and biometrics and linking these to their electronic credentials, either ‘one time’ for a single transaction, or permanently. They may also be required to ensure that there is nothing in the design or operation of their identity scheme that excludes or prejudices any individuals or groups. Identity providers also have a responsibility to ensure the integrity, confidentiality, availability and non-repudiation of whatever identity data they hold. They will need clear accountability for their policies, processes, staff and actions in relation to identity management, with codes of conduct, guidance and associated training. They may need to repair an individual’s identity information, where registration or cross-references to credentials have been compromised or mistakes identified, with fast corrective action. They may also be responsible for redress to the identity subject, if compromise of individual’s identity is their fault, again, with fast corrective action. In every case they will have responsibilities specified in contracts with relying parties (which will differ widely according to the level of identity assurance they are offering, the use and purpose of the identity authentication and transaction(s) involved).

In addition, identity providers should not give to others or use the personal data associated with personal identity without the consent of the identity subject except for defined legal purposes (principally national security and countering serious crime). This means that identity subjects must be given the choice of opting in to plans to extend access to new relying parties or share their personal data beyond what they agreed to at the point of original data capture, unless there are overriding lawful reasons for this extension. This is partly, but not wholly, covered in the UK by the Data Protection Act and in other EU countries by their own (marginally different) interpretations of the EU directive on this subject. However, definitions of consent and sharing remain complex and ambiguous. There is a lot of secondary legislation and hidden ‘terms of service’ that erodes these rights.

Relying parties will have rights and responsibilities that will vary according to the service context and contracts.

A key and often forgotten set of responsibilities are those of an identity subject. Identity subjects have responsibilities to provide accurate data to the identity provider in the context of the level of security required by that provider and to assist in the maintenance and repair of that data as it changes over time.

Identity subjects should also have rights to hold multiple identities, anonymity if they wish, to have access to the personal data held by providers and to redress if they suffer harm because of failures by identity providers or relying parties.
The areas the IAWG felt needed exploration in association with this issue were:

- When we identify someone, we sometimes want to establish that they are a unique biological being as recorded on their birth certificate and sometimes that they are the same ‘persona’ who did something at a different time. What are the implications of this for the successful running of a multi-level identity assurance scheme?

- How can an individual control access to their biographic data (and biometric data) after enrolment in an identity scheme?

- What responsibilities should the citizen (identity subject) accept to ensure the identity assurance information held by the provider remains accurate and ‘current’?

**Minimising access and controlling privacy**

It is of interest to consider the perception of the identity subject to the various uses of their identity and, in particular, to the thorny subject of consent for use of that identity and, potentially, the risk of revealing personal data. The concept of consent and its definition differs between countries. The IAWG’s approach to this has been to identify four broad categories of consent and, at the considerable risk of the outcome being sweeping generalisations, the IAWG concluded that there were useful distinctions that could be drawn out in further analysis.

The first category considered was the attitude to consent in public sector transactions: in general it was thought citizens, in non-repressive regimes, were content that there was no bad intent by public sector organisations with respect to their personal data and that any use that was made would be informed and necessary. It is becoming obvious that this level of trust is not as strong as it used to be because of some very high profile data leaks, but it can still be a useful generalisation and it would be relatively easy to recover a high degree of trust in non-repressive regimes.

The second category of consent considered was that associated with law enforcement and, by extension, to issues of national security. It might reasonably be held that these are not exactly the same with respect to the need for consent, but there is sufficient similarity at the level of serious and organised crime, and terrorism, to enable a broad equivalence. In this instance it has been posited that the identity subject does not expect to give consent and certainly is not asked to give it by the agencies involved. In general, the IAWG believes that this is true although the level of contentment with the status quo might decrease in the face of obvious abuse, and does not exist in repressive regimes.

Thirdly, the status of consent with respect to commercial transactions was considered. This is an interesting case because in Western countries, it is the most highly regulated to ensure that consent is obtained, but, until recently, this has been at least partly negated by the use of very small print, opt out rather than opt in and voluminous (and therefore not read) consent statements. Notwithstanding this, the balance of need – the customer’s to obtain their purchase and the commercial entities’ need to retain their reputations – tends to ensure that an appropriate balance is achieved. This situation can be expected to improve as the consumer becomes more aware of the potential for misuse of identity and personal data. However, this is an area where identity data is expanding fast (for example the increased use of positional data for targeting advertising).

The final category is identity in social interactions and is, in particular, related to social networking mechanisms. It might be thought that this case would be very similar to the commercial transaction scenario but, because something that people want is being offered at apparently no cost, no thought is usually given by the user to the business model of the provider. As a consequence of this and the feeling of the user that they need to participate in order to be in the social groupings that they desire, the users have a tendency to worry even less about the terms and conditions under which they give consent. Indeed, it is only very
recently that there has been significant kickback against social networking sites for loss of privacy and the risks of identity theft. A recent additional phenomenon in social media is impersonation. Increasingly, high profile individuals are being advised to establish at least a minimal presence on social networks to avoid the creation of ‘spoof’ profiles being set up by others to their detriment.

In addition to the risks and issues connected with consent there is the fact that there is just so much information about any individual ‘out there’. This means that there is a market for the ability to draw a large enough number of these repositories together to produce data that is very meaningful for the organisation doing, or commissioning the aggregation. This could be for good motives or bad, but even when the motives are good the outcome could be less so.

The initial thinking of many agencies about identity management and assurance was to put all of the data in one centralised database and protect that one database really well (see Figure 2.1). This thinking was very popular with governments for their schemes for the use of identity information for many purposes ranging from national security and counter-fraud to making life simpler for the citizen when dealing with bureaucracy. However, there was a level of mistrust about the unnecessary aggregation and retention of much more data than was needed, for example for a simple transaction, and it was also realised that security is always only as good as yesterday’s knowledge and that, once security was breached the data loss could be enormous.

Figure 2.1 Centralised database

Figure 2.2 indicates a potential way in which these problems may be being overcome. In this instance the middle entity is intended to represent multiple data stores rather than a centralised database. Moreover, the notion of only having a one-way flow of identity information is introduced. This is in addition to the further notion that those entities that need the identity information only get as much as is needed for the category of transaction being undertaken. In this approach identity data can only be verified with the correct permissions and only to the extent necessary for the purpose. Much work on this is going on at the moment, especially in Government circles and internationally, for example at the European Commission level and in International Standards bodies.
These considerations lead to a discussion of how to ensure that organisations in this field can incorporate the need for privacy in their culture. The need is to ensure that clients’ privacy needs are properly addressed from initial system proposals through to end-of-life decommissioning. In this context organisations must balance ‘need-to-know’ against ‘need-to-share’ to protect clients’ privacy. The use of privacy enhancing technologies could assist, but, in general, these tend to be conceptually difficult and mathematically abstruse, and thus are not easily accessible to the general public and business decision-makers. These issues are not near to being resolved yet, but should be a central part of any solutions adopted.

The areas the IAWG felt needed exploration in association with this issue were:

- How do organisations balance ‘need to know’ against ‘need to disclose’ so this is an internal organisational and cultural issue?

- How do organisations establish a culture of privacy to insure that client privacy needs are properly addressed through the life of that data, and so that it includes decommissioning which is often forgotten? and

- How can the conceptually difficult and mathematically abstruse ideas of privacy enhancing technologies be made accessible to the general public and perhaps more importantly to business decision-makers to enable the previous two issues?

**Registration authorities and ID assurance**

The management of digital identity involves five processes: registration (enrolment); authorisation; authentication; access control; and revocation.
The most important aspect of any identity management system is the registration process. The key is ensuring the person claiming an identity is the rightful owner of that identity and it is not stolen or fictitious. It is also important to ensure that once registered with that identity the person cannot register further multiple identities. However, personas can be registered and may be linked to the primary identity. Ongoing management of digital identity then involves other processes, such as authentication, credential management, change of circumstances and revocation. The organisation, or part of the organisation, that registers identities is normally called a registration authority.

Without effective registration, irrespective of how good the system is at maintaining integrity, it may lead to an easy method to steal identities or commit fraud. In the design of one large identity management system, a lot of work has been done on what sort of data you really need, what sort of data exists about a person and how can it be corroborated. The fundamental question is: how do we really know who any of you are?

With individuals there are three main sets of data (see Figure 2.3):

- **Immutable attributes** – those that can never change. This includes things like who are your biological parents, what your gender was at birth, what your actual date of birth is. These are facts or registration of actual events and can even include certain biometrics such as iris colour and pattern.

- **Assigned attributes** – these are the facts that are actually recorded and become the truths about a person. These can be your recorded date of birth, rather than your actual date of birth. It can include your gender now, rather than your gender at birth, your parents rather than your biological parents. These sets of attributes and data are the ones that people rely on. The assigned attributes are the ones that people in government and in most of your interactions use. So they tend to be the most important.

- **Related attributes** – those attributes that are not part of your identity but are related, such as address, relationships, work interactions, social interactions, financial interactions, qualifications etc. The organisation needs to record the pertinent attributes for each relationship you have.

*Figure 2.3 Attributes of an individual*
When a registration authority puts an individual on one of these databases, the first thing they need to work out is whether or not that claimed identity actually exists. They take all of the attributes and claims asserted by the individual and work out if it is a real identity. Is there evidence that it exists in society, are there interactions that can be corroborated by independent third parties, does it have any gaps in its history? The process is shown in Figure 2.4.

**Figure 2.4** Does the claimed identity exist?

- The claimed identity exists
  - Evidence it exists in society
    - Unique ID creation events exist
    - Attributes can be corroborated
    - Claimed events can be corroborated
    - There are no unresolved anomalies
  - Evidence it exists in history
    - No evidence of death/non-use
    - Identity used recently and regularly

REGISTRATION AUTHORITY HAS TO ESTABLISH CLAIMED IDENTITY REALLY EXISTS

Then they need to work out whether it belongs to the claimant. Is it their identity, or is it one they have made up or one they have stolen? Is it unique? So they will go through a number of processes to make sure the identity exists, it really is their identity and all of those attributes asserted are really associated with that identity. This is shown in Figure 2.5.

**Figure 2.5** Does the identity belong to the claimant?

- Claimant owns this identity
  - Provenance can be confirmed
    - Person matches biometrics
    - Person has original documents
    - Person knows the history intimately
    - Identity not been claimed before
  - Identity matches profile
    - Claimed gender/ethnicity/origin fits
    - Claimed attributes consistent with ID

REGISTRATION AUTHORITY HAS TO ESTABLISH THIS REALLY IS THE PERSON’S IDENTITY AND THEY ARE NOT TRYING TO STEAL IT OR CREATE A FAKE ONE

Then comes the important part: immutably linking the two together (forming a bond between the identity and the individual that is very hard to break, very hard to subvert and makes things like identity theft much harder). This is shown in Figure 2.6. One thing to note here is that biometrics (fingerprints, photos etc.) are not just personal attributes that can be used to corroborate an identity, they are also very good credentials for forming a link between the identity and the person. This is why photos are used on the passport and driving licence.
There are important differences between types of registration authorities. Government needs to know your real identity, they need to know you are who you claim to be, all the way from birth certificate through to where you are in your life today. If they are going to give you a passport, if they are going to give you benefits and protect you as a national citizen, if they’re going to tax you, they need to know who you are.

So it is essential to be clear about what level of identity assurance is needed and recorded and the information should be included for each of those levels.

The areas the IAWG felt needed exploration in association with this issue were:

- What is a core identity? What attributes make it up?
- Should biometrics be used?
- Who should have the authority to register a core identity?

Rights and responsibilities of ID providers

If you go into a shop you have a consumer right, when you pay for a product, to expect that the product works. The shop has the responsibility that if the product does not work you can take it back and get it changed. Figure 2.7 illustrates this in the context of identity provision.
It should be noted that the service provider may be providing services 24/7, so that service provider needs to get 24/7 support from the identity provider. The identity provider could be either a government or a commercial organisation, such as a bank. For example the customer could be paying a local tax to the government using their credit card. In that case the user would be using the bank as the identity provider.

The identity provider really has a right to make sure the information given to them by the registration authority is correct and, like the individual, they need to get redress if something goes wrong. The chain has got to work all the way through, as illustrated in Figure 2.8. In this example there are multiple providers of identity. There is a portal, between them and a service provider, and a number of attribute providers down the bottom. The user may be going in through any one of their identity providers, maybe their bank, via the portal, which is a managed service. If you are paying your tax using your credit card then the only attributes of interest are your tax account number and whether the credit card has the available credit to cover the tax.

The areas the IAWG felt needed exploration in association with this issue were:

- How do individuals gain trust in the process?
- How can we ensure the individual persona is who they say they are when they request a service, and if something goes wrong will there be a speedy restitution and redress process?
- Will it be up to the individual to ensure that any information held by an identity provider is up to date and accurate (a responsibility), or is it an individual’s right that the information is correct in the first place? Is it a case of ignorance is no defence?
Security versus privacy: the balancing act

Security versus privacy is often referred to as a balancing act. In reality it is really a case of proportionality because every individual needs to maintain their rights to both security and privacy. It is important to distinguish state security from data security. Without security of personal data, no individual can maintain their privacy. So anyone who wants privacy must also have security. Security is a compromise not a trade off. Total privacy and total anonymity are simply not possible on the internet. Major problems exist if the State apparatus is not trusted by the citizens to look after their personal data.

One of the key success factors of getting public confidence in any identity assurance scheme is to ensure that the information is only available to legitimate agencies for specific authorised purposes and that the data subject is in control of its dissemination. However, to ensure the security of the state it is sometimes desirable for security agencies to have access to information about individuals. At times, for reasons of national security, it may be necessary for the state to do this without the individual’s knowledge. The issue is: how can this be achieved in a reasonable and proportionate way without losing trust in the system or transgressing personal liberties?

This is always going to be a difficult and subjective issue. State security in non-repressive regimes is primarily about protecting life and the democratic process. Personal privacy is about allowing an individual person to protect his or her way of life as long as it does not impact in a negative manner on the lives of others. Article 19 of the Universal Declaration of Human Rights addresses some of the issues, but is it definitive enough?

State security certainly includes counter-terrorism, but what else? Are money laundering and tax evasion, for example, included? Article 19 is not definitive on this issue and different countries interpret the Article in very different ways.

- Who can be regarded as part of the state security apparatus? Is it just the security agencies or does it include law enforcement, military and local councils, for example?
- What information can be made available to such agencies? All of it or just certain fields? Can it be browsed/searched or has the agency to request individual items?
• What is the process for authorising such access? Does it involve warrants, authorisations and, if so, who is empowered to give permission?

• How long can data be kept and what standards for its destruction are needed?

• Is there an audit of the whole process to assure the general public that there is fair play and their rights are not being abused? Does this include checking that no-one has ‘hacked’ the access mechanism?

• Can the individual discover who has accessed their information and when (e.g. if they are subsequently charged with an offence as a result)?

The areas the IAWG felt needed exploration in association with these issues were:

• What principles need to be in place to ensure an individual’s right to freedom of opinion and expression (and why)?

• In the context of identity assurance, what are legitimate national security interests (and why)?

• What safeguards should be in place to ensure that personal privacy is protected whilst not compromising national security?

Identity governance on the internet

There is no global identity management system and there cannot be a single rigidly defined system for all of the reasons already discussed above. Global identity management will have to be a federated identity assurance system and must be pragmatic and adaptable. What is needed at any one time and place is context and transaction sensitive. More and more public services are going online and more and more business is being conducted online. Social networking and the increasing use of positional data mean that identity governance has got to be understood, discussed and enabled. The impact of legislation in relation to internet issues is highly unpredictable. Things are changing very fast. So, identity governance on the internet is important for the confidence of all participants and must be agreed globally.

There is no central governance of the internet. Many organisations are already involved in internet governance, for example the United Nations, the Internet Society, the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), the Internet Assigned Numbers Authority (IANA), the World Intellectual Property Organization (WIPO) etc.

It is important to be clear about principles and responsibilities, rather than trying to put in place regulations and legislation that is technology specific or specific to a particular point in the development of these new ways of using communications and doing business. There is no central control of the internet.

There are also many drivers of identity on the internet which are ever more complex. In day-to-day life people are making choices that are based on the assumption of knowing who they are engaging with. This raises many questions for identity governance within the wider issues of internet governance. These issues revolve around questions of standards: control versus federation, and processes and liability flows.

Any discussion of identifiers has to consider both policy and the supporting technology. They do not exist independently of each other.
Aspects of Identity

The internet environment relies on IP addresses. These are related not only to actual address owners, or users, but also to all the resources on the internet, including: people, things, applications and computational services. Over time there will be different identifier systems. So internet governance has to deal with some of the issues of interoperability. One type of identifier is a binary string that exists on a network, but another way of identifying people is by virtue of identity credentials, such as a private key. When you use a private key to authenticate yourself to someone else, or you use someone else’s private key to authenticate them to you, all you are doing is saying that you trust that the party that you are dealing with is the party that currently holds the private key. So you get another layer of mapping that says who this private key is assigned to and who had the trust to do that mapping. But for that trust to be well placed, you also have to assume that the ‘end point’ (the device that the identity subject is using) and other devices in the system have not been compromised.

Somebody has to make an assertion about authenticity. You trust that they made the correct judgement, but, more generally, it is probably going to be an organisation that is going to do a more in-depth analysis. Most governments, when they give credentials to their employees, do background checks. At high levels of security clearance, they talk to members of their family, friends and relatives and they might even do DNA testing. The very first questions that come up are: to what extent can information about this identifier be made known publicly and to what extent can most information about the identifier be kept private? Along with that comes the question of the extent to which anonymous identity can be sustained in the internet environment and for what purposes.

Good meta-level structures for dealing with not only identity, but all the mechanisms that assure that the identity is valid are needed in internet governance.

For federated identity, which is the only practical system, the important issues are anonymity, pseudo-anonymity and attribution, at various levels as and when necessary, in the context in which you are operating. In every transaction it is necessary to consider: what are the risk or threat models that you are operating under? There are three stages for identity assurance: authentication, authorisation and audit. Authentication is about whether an individual has a credential, such as a passport. A passport is a federated credential that is acceptable in any country as a form of identification. The vetting that is necessary for the production of passports is federated. Each country is allowed to issue passports. It is their responsibility to make sure that the identities are, in fact, correct; that it is a valid document and it ties to a real (biological) person. Passports work well in the real world. On the internet individuals and organisations are operating in a virtual world. In the business world, if you are going to have a federated system you have to have trust in the credential, produced by the identity subject or from the identity provider, on the relying party side. In business transactions you also need to know the flow of liability. If you think about the credit card industry, you have the issuing bank for the card. The liability flows from one transaction to another and it is always known where the liability rests.

There are interactions on the internet that require no attribution and where anonymity should be preserved. In the USA, this concept was a very important part of the founding of the country: the right to speak anonymously is embedded in the US Constitution.

Internationally, there appears to be a clash between privacy, which is a European basic principle, and openness, which is a US basic principle. However, the two systems can interoperate and do interoperate or operate in parallel. These types of international differences are much greater between repressive regimes and democratic governments. While human rights are universal, the way that corporations and technologies function in the contexts of repressive and open regimes is very different. This may mean that what is a good technology, or a good internet governance approach for the free world, or even the partly free world, has very different uses and consequences in a repressive country. In a repressive regime anonymity is going to be far more important to individuals. If there is to be an internationally agreed identity architecture, it needs to be workable in all regime types.
The areas the IAWG felt needed exploration in association with these issues were:

- Who would be appropriate to determine the frameworks for identity governance on the internet? The United Nations? (Such a top-down bureaucratic approach has already been rejected in the UN IGF process.)
- Who could have the remitting authority?
- Is the identity assurance framework a question of control or a question of standards?

**Trust in transactions with remote identities: anonymity, pseudo-anonymity and attribution**

The remote identity problem is mainly a product of the internet. Legacy remote identity assurance is an accepted risk. Figure 2.9 illustrates this through the example of an ATM transaction. Most people trust this type of transaction, even remotely, because it involves trusted credentials and a trusted infrastructure.

**Figure 2.9** Legacy remote identity assurance

![Figure 2.9 Legacy remote identity assurance](image1)

The difference that the internet makes is illustrated in Figure 2.10. With the internet we not only have an untrusted infrastructure and an unclear legal framework, we often have difficult-to-trust credentials and unknown (or only trusted by reputation) correspondents at the other end of our transactions. Solutions to this situation are likely to be complex and difficult to implement but are essential for full use of the power of the internet.

**Figure 2.10** Internet remote identity assurance

![Figure 2.10 Internet remote identity assurance](image2)
Take, as an example, the issue of anonymity. It used to be said that on the internet nobody needs to know who you are (the joke was ‘nobody knows that you are a dog’). In addition to this not being sufficient for most transactions going forward it probably isn’t even true these days (it is likely that, for example, the social network providers not only know that you are a dog, but also know that you are a Dalmatian with 101 spots and a neurotic owner).

The IAWG considered that the four key questions which arose from these considerations are:

- How can we effectively check an identity remotely over the internet?

- Will it be possible to use the same kind of secure and reliable credential for everyone? This would be ideal but, as examples, what would be the impact of various forms of disability or people who are monolingual in a minority language?

- How can non-repudiation or other forms of accountability be achieved?

- How can identity theft and fraud be prevented, especially during registration?
3 Ways forward

When considering identity assurance on the internet, it is important to remember the latter’s evolution.

Thirty years ago, phones were fixed. Then mobile phones started to be used for one-to-one conversations. You decided who you wanted to call and you usually recognised the voice of the person you were talking to. You knew who they were and you knew that you trusted them. If you rang your mother, you knew it was your mother answering the phone because you recognised the biometric of her voice. In just the same way on the internet over 20 years ago the users were a limited group of people in a small number of organisations, and so it was trusted by all involved.

Initially the internet was an extension of what people had been doing for years. Now, the internet can link everyone and everything. In 2010 there were an estimated five billion IP-based devices in the world, growing to 15 billion by 2015, linking over half of the population of the world. There may be ten times that number of ‘smart tags’, such as radio frequency identification devices (RFIDs). Now you cannot know, let alone trust, all of these people and things. The greatest vulnerabilities now concern mobile access and embedded systems. You may think you know whose phone you are communicating with, because the name and number of a friend pops up on your screen. However, a few statistics from the UK give the lie to that. In 2010, over 20 per cent of people lost their mobile phones or had them stolen. More importantly, over 60 per cent of those people didn’t even have a PIN on their phone, let alone any more sophisticated security.

So it is an inescapable truth that you can neither know with whom you are communicating on the internet nor who owns, let alone who is using, the device or the IP address that you are communicating with. However, sometimes you do need to know both of these things. You need to know who or what is at the other end and who they legitimately represent, be it a government or a business, if you want to benefit from internet services and transactions. This is why the management of identity on the internet is so important. Increasingly, you also need confidence in devices you are communicating with (such as smart meters and medical monitors).

Identity governance on the internet

Governments need to have a policy to ensure their citizens have access to a safe and secure internet, to encourage social interaction, and to enable access to content and development. Internet governance is hard within the context of a single country with a coherent culture and set of mores. However, internet governance has to be achieved globally. The UN IGF provides a good forum for dialogue on the issues.
Aspects of Identity

Governance concerns

- Key principles: open architecture; multi-national, multi-stakeholder dialogue; interoperable standards.
- Minimise attribute data for each transaction.
- Are EU data protection laws protectionist?
- Is domain name system blocking and filtering necessary and proportionate?

Only a small number of principles are key to internet governance: open architecture; multi-national, multi-stakeholder dialogue to develop good governance and an understanding of conceptual meta-level approaches to complex networking with the adoption of interoperability standards.

Outside the EU, our data protection laws are seen as a protectionist device and not a strongly held principle, because the key for users in developing countries is that the internet is cheap and flexible. There is also a serious culture clash between US anonymity first and European privacy first that is one of many cultural differences that will have to be respected.

The reality is that users expect their data (including identity data) to retain domestic levels of protection (whatever these may be) whatever jurisdiction they are in on the internet. Common principles and compromises are needed, but these will be very hard to achieve. It is also important to consider processes and liabilities. For this reason more delegates from both the financial and legal sectors need to attend the UN IGF if it is to make real progress.

For individual users the internet is ‘experiential’. Trust increases with use and depends on the national and individual starting points. In developing countries trust rests largely with major companies, such as Google, Microsoft and Facebook. Whereas in Europe there are many privacy concerns about these companies’ data retention policies and commercial use of individuals’ identity attributes.

Some people think that IPv6 could allow every individual to have their own unique identifier to use online and this would solve all problems. However, at the BCS UN IGF workshop, when the participants were asked if they thought people should have one unique identity on the internet or multiple identities, everyone was in favour of the latter. People do not want to be pushed to have one identity. They want a PayPal identity, a Google identity, a government identity, a social identity and so on.

There was a very strong thread at both EuroDIG and IGF that said the misuse of information access and the ability to identify individuals, especially by oppressive governments, meant that online we need the ability for the same individual to be anonymous for expressing opinions and fully identifiable for online banking and commerce. Separating the two can be very difficult. Especially when you consider that concerns about such things as bullying among school children and defamation in blogs, leads to counter-calls for no anonymity by some groups in the UK and Europe.

In online commerce you need to be able to prove that you are able to honour the transaction and pay. However, for legal compliance reasons an organisation you are doing business with may also need to know who you really are. Here we come back to the vexed questions of jurisdiction and how much personal information may need to be revealed to prove identity to access a service.

Most young people from developing countries, and many from Western countries, accept that personal information is ‘commercial currency on the internet’ and this is fine. However, there is a hard core of
privacy rights activists for whom this is wicked and unacceptable. So some people mind about the collection of personal data by commercial companies and some do not, but many do not realise that personal data is being collected and might be connected to their identity.

There is a widely held view by individuals, as opposed to governments and some commercial organisations, that end users should be responsible for authenticating their identity and protecting their personal data themselves (if they so wish) by such means as holding the encryption keys themselves.

In relation to privacy rights, it is widely thought that there needs to be an internationally agreed definition of what comprises ‘sensitive personal data’.

Most people would consider their medical and financial data sensitive personal data. However, a definition of sensitive personal data will be impossible to define globally because the sensitivity of personal data is driven by context. Your address is sensitive if you are trying to escape from an abusive relationship. In some countries trade union or other organisational membership is sensitive personal data because of the nature of the regime. In some circumstances your health data may be sensitive, such as if you are HIV positive. On the other hand, the fact that you had broken your arm as a child, may not be. There are few absolutes. Views vary both between individuals and cultures and over time. Biometric data is often considered sensitive personal data. However, most people accept that use of biometrics can be privacy enhancing. Examples are using a biometric to secure access to your computer or phone or enabling doctors to use facial recognition to open shared computers on wards so that only those authorised can see medical data and access is denied as soon as the authorised individual walks away from the screen to attend to another task.

The European view, as expressed by the Council of Europe via EuroDIG, that puts human rights and net neutrality, as absolutes, at the top of the agenda, without due consideration of the proportionality between security and privacy is not a governance model that is widely accepted outside Europe.

There are big differences in the governance needs in repressive societies and free, open societies. In repressive regimes anonymity is much more important, but it still cannot be maintained in commercial transactions.

Ways forward on internet governance could be achieved via:

• corporate social responsibility reporting in company accounts;
• international conventions that countries could sign up to;
• consumer protection agencies, because most countries have these and many countries already have bilateral and multilateral agreements across borders that could be developed for internet trading.

Another possible governance model would be multilateral template treaties.

**ID for ecommerce**

Identity assurance at some level is vital in connection with business transactions over the internet. You need a degree of certainty about who the other party is, 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 to or from your bank related to your bank account.
In business, understanding the flow of liability is vital. You need attribution before doing a commercial transaction. You need to know who is backing a payment. One element of trust concerns whether you as an individual or business have adequate means of recompense.

In business you must trust the other party. When you are doing a business transaction you do not want to do it with an anonymous person or unknown organisation. You want to do it with a trusted party and you want redress if it goes wrong.

As an individual you also want to know to whom you are handing over personally identifiable information, so openness for people engaged in commercial transactions is essential.

It is also vital to distinguish between an individual consumer doing business and an organisation. If you are doing business with an individual, you need to know who it is and that may 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 that transaction in the organisation, per se. There is no justification for the relying party insisting on a personal ID for the individual acting on behalf of the organisation.

In financial transactions, credit checks and fraud prevention are all about context. ‘This transaction seems unusual from this person with this history, suddenly coming from this geographical region in this context’. However, the degree of granularity in those checks is a major concern. Both the business, for its own protection, and the customer for confidence to transact online, need an optimum balance between false positives and false negatives either preventing a genuine transaction or blocking a fraudulent one.
Commercial models on the internet

• You may need to pass trust from one system to another.

• Trusted third parties may be part of the solution.

In considering financial and commercial models in ecommerce, you may need to be able to pass trust from one system to another. Roaming is allowed on mobile phones. It works because the phone companies are obliged to accept the identity and payment agreements of individuals registered with other companies. This is an excellent example of trust over federated networks. Payments beyond just the contractual payment for phone use can also be added to a mobile device.

The transfer of money (mainly in small amounts) on mobile phones is becoming very important in many developing countries including Kenya which has M’pesa (M’pesa in Kenya works as the mobile phone company accepts the liability for small payments on the mobile chip). This is bypassing the whole bank credit and debit card systems established in the West. It is an excellent example of the successful use of trusted third parties on the internet.

Trusted third parties will almost certainly be part of the solution in ecommerce over the internet.

ID for egovernment

There are three aspects to identity for egovernment (see Figure 3.1). These interrelate and in some places overlap, but are normally kept separate because they have different business objectives and in many cases are covered by different legislation and policy. The first is citizen interactions with government, including provision of services to the citizen via the internet. The second is business interaction with government, which can also include supplier interaction, but more normally covers businesses meeting their regulatory requirements. The third is employee interaction, which for obvious reasons has much more stringent requirements on identity and authentication.

Figure 3.1 Identity for egovernment
Aspects of Identity

This section is based on the UK Government scheme of federated identification management, but the points made apply to a variety of different schemes adopted in other countries.

The key difference between citizen interaction and employee interaction is that the citizen authentication is balanced around privacy and data protection, and (in some respects for the same reasons) employee authentication is balanced around accountability and being able to trace every action to an accountable individual. One of the key things they have in common is to reduce the cost of providing services and the cost of ICT to government and the wider public sector (e.g. health, police, education).

For the citizen it is about providing services online, so that they are available 24/7 and are easy to use, in most cases from any computer connected to the internet. The eventual aim is that most services, from renewing a tax disc to making a doctor’s appointment can be done online and will be ‘digital by default’.

For access to many government services in the UK at present the citizen is asked for personal information, either to identify them or to find their records in the department they are communicating with. With the future federated egovernment model, the goal is to have much less personal information moving around and to put that back in the control of the citizen wherever possible.

Work is under way in the UK to develop a federated identity management system which can be implemented by multiple organisations, both private and public sector. They will have to meet stringent standards and be certified to operate as a registration authority or identity provider, but in effect any organisation could become certified. The citizen would then register with one (or many) registration authorities and use multiple identity providers to interact with government. The identity providers would handle the personal information required for identity validation to the level required by the services to be accessed.

For employees things are different. Gone are the days when someone went to work for a big government department for 43 years of their life. Now people move between departments, work remotely and in some cases work for suppliers where government has contracted out services. However, government has a responsibility to protect information and handle it with care. This is not just for national security reasons, though this is part of the requirement. It is more about ensuring staff handle citizen data properly, protect personal information and only use it for the purpose for which it was collected. It is also designed to ensure that staff follow the proper procedures and can be held accountable for mistakes and unauthorised activity.

As a result stronger access control systems with better authentication methods are required supported by better auditing and accounting of activity. This also acts as a deterrent to those who may consider abusing their position.

Work has not really started on better registration and authentication of companies and other organisations, but this is expected to start in the UK in 2012.

In all cases BCS is involved in both contributing and reviewing the deliverables from these programmes of work in the UK Government and will continue to contribute during 2012.

ID to combat ecrime

Whilst many aspects of ecrime are dealt with under previous headings, one remaining large field is that of illicit (or illegal) content being made available online. This content takes many forms and its ‘illegality’ is context dependent. For example, there is widespread consensus over the unacceptability of material showing child abuse and limited concern over prohibition in Germany of material glorifying the Nazis. Chinese prohibition of material supporting the Falun Gong is seen in the West, however, as a limitation on
free speech. At the other end of the spectrum is the widespread but unauthorised distribution of material which is not in itself illegal, but which is supposed to be protected by copyright. The copyright owners consider this unauthorised distribution to be a straightforward theft of their rightful royalty payments which has given rise to the concern that an undermining of the copyright system will stifle artistic creativity. Those who engage in this illicit sharing of material equally forcefully argue that copyright periods of the order of ‘life + 70 years’ has more to do with preserving the outmoded business models of large corporations than it has of protecting artistic creativity.

A common response to these problems by national governments has been to censor the internet sites illicitly hosting material, often by manipulation of the domain name system (DNS). An alternative sometimes used is the blocking of IP addresses either to prevent access from a group of IP addresses or prevent access to a group of IP addresses.

But DNS filtering and blocking are blunt tools that can often be circumvented through the use of anonymising proxies. An excessive focus on illicit or illegal online content may itself impede creativity, foster criminal activity and damage innovation on the internet. It can be argued that by attacking the content via IP addresses, law enforcement agencies are blocking consumption, driving services underground and bringing only short-term relief because the content just reappears elsewhere. If content is illegal, it may be thought that law enforcement should find and prosecute the perpetrators not block the sites.

DNS filtering is widely seen by those in developing countries as stigmatising the majority of legitimate users because, 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.

Requiring identification to be presented before going online is sometimes proposed as a solution to this problem (because it would allow law enforcement officers more easily to track down those who access illegal material) but such a requirement, combined with the required monitoring of online activity, seems intrusive, difficult to implement and very disproportionate. The issue being the identification of the user rather than the access mechanism (e.g. think ‘free’ WiFi access, ‘Pay As You Go’ mobile and internet cafe style access).

One area that might warrant further attention, however, is more rigorous identification of website owners, to encourage greater cooperation with local law enforcement to ‘take down’ illegal or illicit material. While the current domain name registration system is designed to enable such action, the rigour with which identities are checked leaves a lot to be desired in many jurisdictions.

**Issues of privacy and security**

If an individual is given total privacy and the ability for complete anonymity this can give rise to major problems, not only for state security and law enforcement (e.g. to protect against terrorism), but it will also place a large burden on commerce and government doing business online. Indeed, it could be argued that total privacy is impossible to achieve. On the other hand, if state security uses the information for purposes other than their specific role, then this is likely to cause issues for the individual. Everyone requires a level of security both to the information and the use to which it is put.

So as a starting premise, privacy is good and security is good, however the relationship between these two is not linear because too much security, while leading to increased privacy, can adversely impact on other areas of a person’s life. An example is a person’s medical records: these should be private but need to be available to not just a person’s GP, but to hospital staff should the person require emergency medical care. So there is a need to balance not just a person’s privacy requirement against security, but also against the need to make certain elements of a person’s private data more widely available in a controlled way.
Aspects of Identity

Where do you start in assessing proportionality? It is our contention that the starting point has to be a firm understanding of what information is being held, where it is held and for what purpose. The ‘what purpose’ is key because this will help to identify information that, whilst being private, needs to be available to one or more bodies or organisations other than the individual. For example, bank account details, whilst private, are held by a person’s bank because without these, the person would not be able to conduct banking business. Likewise medical information will likely be held by the local GP, but would need to be made available to a hospital should treatment be needed.

With a firm understanding of ‘personal’ information, its value can be assessed and together with the location, purpose and sharing requirements, the associated risks can be determined which will lead to the identification of a required level of security. With knowledge of the required level of security and the technology and media used to store, process and transmit the (personal) information, an appropriate set of controls can be defined.

In short, we need to explore and document the safeguards necessary to achieve proportionality between the individual’s right to privacy without compromise and permitting lawful use of individual data.

As emerged in the previous chapter, it is over-simplistic to assume that privacy and security are opposing forces or that a ‘balance’ has to be reached between them. Rather, the balance to be achieved is between the rights of individuals as individuals, and those of individuals as members of a larger group. This again is highly context dependent, varying not just between different states or cultures, but also at different times within the same group, and dependent upon different individual circumstances. In Western democracies there is an emphasis on individual rights, such as protection of personal privacy, but individuals will cede some of those rights in return for healthcare or welfare support or the rule of law which society provides. They may allow greater infringement of individual rights if there is a perception that the threat to society from, for example, terrorism, has increased, or they may wish to claw back individual rights if their trust in democracy and the rule of law is lessened. Similarly, individuals may cede some rights to privacy to commercial entities in return for provision of a service that benefits the individual, but again, as we have seen for example with Facebook, individuals will want to claw back those rights if they feel that they are being unfairly exploited.

Other cultures may legitimately set a different balance point between the rights of the one and the rights of the many. But serious problems arise when those charged with setting that balance point are seen as unrepresentative of society as a whole, such as during the Arab Spring uprisings, or are using their power to discriminate against, or to persecute, sections of society.

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). And it must ensure that the benefits the internet can bring are not stifled by an over-strict control on who can connect.

Commercial exploitation of identity

By the autumn of 2010, Facebook was running more than 60,000 servers, consuming over 10 MW of electrical power to serve its 500 million+ users. The stock market appears to be valuing Facebook at more than $100 billion. Google is valued at about $175 billion and operates over 450,000 servers, costing perhaps $2 million per month for electricity charges alone. In 2010, Google was responding to 34,000 searches every second.
While these examples are extreme, more and more businesses are offering low-cost or ‘free’ services to internet users. Yet these services are clearly of value to the provider as well as the user, and equally clearly must be paid for somehow. The value to the provider, of course, derives from the information these services gather from their users, which may then be used to tailor or target revenue-earning advertising and services at them. This information may be about purchasing preferences, hobbies, geographical location, friends and family, political affiliation, entertainment interests and so on. In short, any and all components of a biographical identity may be discernible.

Individuals obviously derive enormous social and economic benefit from such services. Indeed, it is hard to imagine what the internet would be like without search engines such as Google. And it is equally obvious that companies that are investing in, and operating, these services must be able to make a profit on their investment, because it is this that is driving innovation on the internet.

But there are serious concerns too. Do the users know what information is being collected? Can they control what information is gathered? How can they give consent to its use? Will they be subject to overt or covert discrimination on the basis of the information? How is it being protected? How, and to whom, is it being disseminated? Can the information be used for malicious or criminal purposes?

As data mining continues to grow in scale and sophistication these issues of the commercial exploitation of identity information will intensify, and merit much further study.
4 Conclusions

A wide variety of views was expressed at the different forums to which the IAWG presented in 2011, but the fundamental differences stemmed from participants’ assessment of the importance or otherwise of identity assurance in determining individuals’ rights to security and privacy.

Participants at Infosec were security professionals – many from overseas, mostly young. They understood the complexity of the problems and were keen to discuss technical solutions. They generally accepted the importance of electronic identity assurance and were inclined to think that security trumped privacy, but it was technically possible to have both.

Many of the delegates at EuroDIG were human rights and privacy advocates and a vocal minority regarded a free internet and free content as their human right. This minority was unwilling to concede that if they did not pay then someone else would have to pay for it with their privacy. The view expressed at EuroDIG was overwhelmingly that privacy and anonymity trumped everything else.

At EuroDIG three recent surveys about principles for internet governance were mentioned. One had been conducted by the Council of Europe. It reported that human rights were the core principles. One by the OECD said economic development was the core principle, and one by NATO found security was the core principle. These surveys seem to represent the views of the survey organisers, and presumably reflect both the survey’s wording and the views of those attracted to respond to them.

The delegates at the UN IGF, which was by far the largest meeting, were:

- parliamentarians;
- government officials;
- internet registrars (such as Nominet);
- law enforcement (including criminal justice and judiciary mainly from the USA);
- business (largely the IT sector majors, such as Microsoft, Google, Cisco, Nokia);
- some smaller (mainly African) businesses; and
- civil society (largely human rights, privacy and freedom of the internet activists, as at EuroDIG).

At IGF, the ‘EuroDIG’ view of putting human rights at the top of the agenda, followed by the internet as an open free space, without proportionality between security and privacy was not widely held except by some
Conclusions

of the European delegates. It was stated in the concluding session that governments need to have a policy to ensure their citizens have access to a safe and secure internet, to encourage social interaction, ensure access to content and boost economic development.

It was clear that views differed according to the starting point of individuals and groups. The reality is that users expect their identity data and consumer rights to retain their domestic levels of protection (whatever these might be) whatever jurisdiction they are in on the internet.

We draw the following conclusions from these debates:

Views of the internet reflect societal background

Despite the astonishing growth of the internet and its capacity for enabling change, it is important to remember that the internet is just a medium. It can be used for good or ill. People can organise good things or bad things over the internet. Judgements of what is good or bad will vary between individuals, organisations and governments and over time these views are likely to evolve.

For individual users the internet is `experiential'. Who trusts whom depends on the national and individual starting points. These are very different for users from different countries.

For example, in most developing countries users are using the internet principally from smartphones for social and entertainment reasons. The users trust the big name companies such as Google, Microsoft and Facebook and are largely unconcerned by any privacy issue. If user’s costs can be kept low through data mining and advertising, this is what they want.

Most people in developing countries have skipped the fixed line internet experience that those of us in the UK started with. They have also skipped the mass use of credit and debit cards, which affects ecommerce.

However, there are many interactions on the internet that require no attribution and can be anonymous. Indeed, in the USA, the ability to speak anonymously is embedded in the Constitution. Interestingly, it was the ability to retain anonymity that was the major concern of delegates who had been involved in the Arab Spring or who came from countries with repressive regimes. In these countries, the privacy concerns that some Europeans hold in relation to businesses were of lesser concern.

Identity doesn’t just apply to people

Identifiers on the internet need to be kept separate from technology. You need identifiers for users (be they individuals or businesses) and things and other resources such as applications.

When it comes to the ‘internet of things’ it remains critical to have trustworthy identifiers associated with them (just as it can be for individuals) in order to know you are getting the right data from the right place (the right online shopping site, the right sensors, the right medical diagnostics and so on). You also need to be certain, in some contexts of use, whether the identifier is immutably bound to the thing of interest or not (such as RFID tags applied to parcels in transit or manufactured into items of value). Just as in some circumstances you need to know the root identity of the individual. BCS intends to take up the questions raised by the ‘internet of things’ in a separate work stream. BCS has joined the UN IGF Dynamic Coalition on the Internet of Things for this purpose.
Aspects of Identity

**Required levels of trust and assurance depend on context**

There is no simple answer to identity assurance on the internet, because what is important depends on context. Digital identity management does not offer a binary choice between full assurance and no assurance. It offers a range of levels of assurance that must be aligned to the risks of the interactions between the parties involved. What identifiers do you need and how certain do you need to be about the use of those identifiers? The highest level of privacy protection that technology enables, consistent with the appropriate level of assurance, is critical to developing the market for online services (especially for higher value or higher sensitivity transactions). Proportionality between privacy and security online is vital because of the capacity of information systems to store identity information and transaction records indefinitely.

How tightly those identifiers need to be bound to people, organisations or things in the real world depends on what you are doing. You need to look at the context of interactions and the risks in the context. Anonymity, pseudo-anonymity, attribution and trust all matter to different degrees to different people in different contexts. However, we have reached a point in the ubiquitous low cost internet, when all users have to accept that personal information (including identity data) is commercial currency on the internet.

**A framework that promotes cross-border trust is needed**

As the internet economy grows, the proliferation of identity credentials and the complexity to individuals of managing these has risks. Identity provision could become an anti-competitive impediment and a point of security weakness. If digital identity credentials are not internationally recognised, this may inhibit high-value cross-border transactions. A key element of such a framework is the capability for law officers to track down and prosecute those who commit and organise crime on the internet. It is harder on the internet than it is in the physical world, particularly as you cross borders, since the pace at which such a capability has to operate is much greater, because transactions can be very fast and at very large scale.

Critically, any such framework will need to be flexible enough to encompass the wide variety of approaches to rights and responsibilities of individuals, business and states that are found across the globe. The processes and supporting technologies that establish and maintain identities, and that provide correction and redress, will all need to be trusted to the extent that transactions warrant.
5 Recommendations

The sixth UN IGF saw some progress in how to enable the internet to aid development and bring economic benefits to all, but it is still in the discussion stage, and business (particularly from the finance sector such as credit card companies), many parts of law enforcement and the judiciary and entrepreneurial start-ups were all under-represented.

The time is ripe for the whole spectrum of law and legal professionals, international finance, phone companies and businesses to make inputs to identity governance. There is an urgent need for the development of pragmatic models that build on the successes of federated trust in international banking, international use of credit and debit cards and international use of phones. In all of these areas individual consumers and businesses have a relationship with local or global companies who they trust and who are able to carry out transactions over the internet, with liabilities clearly articulated in contracts and understood by all parties.

We recommend that the IGF commence work in this area, and BCS intends to continue its work on this vital global initiative of federated and trusted identity governance.

We also urge greater involvement from the financial, business and the wider legal sectors in future IGFs, since it is so important to consider processes and liabilities when we look at assuring identity on the internet.
Annex 1
The IAWG and its activities in 2011 and proposals for 2012

BCS, The Chartered Institution for IT, consulted its 70,000 professional members worldwide at the end of 2010 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 agreed was identity assurance. Trusted reliable identities are needed for the safety and security of citizens and underpin many transactions, particularly where money changes hands or valuable service and entitlements are provided to citizens meeting defined nationality, age or other status tests. In the internet age this means linking identities to electronic credentials.

The BCS Identity Assurance Working Group (IAWG) was formed to examine the governance and other issues surrounding identity assurance on the internet. The remit was twofold:

• To input to the development of citizen identity assurance by the UK Government following the decision of the Coalition Government to cancel the UK ID card scheme. This activity is not covered in this report.

• To discuss and develop the BCS position on this topic more widely. This would result in moderating the position after international discussion and feedback to the Policy and Public Affairs Board. To this end workshops were held at Infosec in the UK, and at the international multi-stakeholder conferences of EuroDIG (Council of Europe Dialogue on Internet Governance) and the UN IGF (Internet Governance Forum).

The results have been fed back to and discussed at the UK Parliament and the Internet Conference and to a BCS/EEMA Thought Leadership Seminar on eID Enabling Business Transactions in late 2011.

The members of the IAWG are Louise Bennett (Chairman), Roger Dean, Ian Fish, Steve Marsh, Andy Smith, Toby Stephens, Peter Wenham and David Williams.

• The Infosec workshop was given by Louise Bennett (Chairman), Ian Fish, Andy Smith, Peter Wenham and David Williams (see Annex 2).

• The EuroDIG plenary session was given by Louise Bennett (Chairman), Ian Fish, Andy Smith, Peter Wenham and David Williams, joined by Marie George (NOOS – France) and Bogdan Manola (APTI – Romania) (see Annex 3).

• The UN IGF Workshop was given by Louise Bennett (Chairman), Ian Fish, Andy Smith, joined by Alun Michael MP, Bill Smith (PayPal – USA) and Robert Kahn (USA) (see Annex 4).

• The BCS input to the Parliament and Internet Conference was given by Louise Bennett (see Annex 5).
• The BCS input to the BCS/EEMA e-enabling Business Transactions was given by Louise Bennett and Roger Dean (see Annex 6).

In 2012, BCS IAWG intends to continue their international dialogue focused on the six areas identified in Chapter 3. Namely:

• identity governance on the internet;

• ID for ecommerce;

• ID for egovernment;

• ID to combat ecrime;

• the proportionality between privacy and security; and

• commercial exploitation of identity.

The first meeting workshop will be at the UK IGF in March 2012 with Eurim, EEMA and IdenTrust.
Infosecurity Europe is one of the largest information security shows in the world, held in London every April. For the second year running, BCS has presented a workshop on identity assurance. In 2010, the workshop was based on the fundamentals of identity assurance. In 2011, a group of presenters from the Security Community of Expertise held a workshop as the first in a series, to ask questions and try to find some answers about one of the topic areas BCS membership find really important.

The workshop was chaired by Louise Bennett, with Ian Fish, Andy Smith, David Williams and Peter Wenham. There were five specific aspects of identity that were covered, one by each of the presenters.

The intention of the workshop was to give brief presentations leading to the questions BCS wished to ask (as covered in Chapter 2). These and other questions were then discussed at round tables. At the end, each table reported back on the key outcomes from that table: both answers and other topic areas and questions that had been raised.

The following is a verbatim summing up of the discussions from the tables at the workshop.

Table 1 (LB) Focus on citizen’s rights and control of personal data

We were supposedly talking about citizen’s rights and control of personal data. I think that some of the key points that came out were first of all that we are in a transitional period, but we do not know what will happen in 25 years’ time. We are not going to be able to speak for another generation. We did feel very strongly that it was important for the government to provide a sensible framework for identity assurance to say that these are the kind of things that a provider should do, if they are going to assure identity to a particular level. But after that we wanted there to be multiple providers that were doing that and we would go to the ones whose reputations we trusted.

But we needed to understand that framework and go to the right provider and one size will not fit all. Everyone agreed none of us wholly trusted government and we came from different countries, so it’s not just a reflection of the UK Government. One of the other major things is to ensure that children are educated in security at an early enough age and really do understand it and the effects on them.

There was a strong feeling that there was a generational divide. We had concerns that our children’s generation did not really have and were not going to have. There would be an acceptance of some things in the future that we find unacceptable now. Trust is not necessarily lost because you have had a data breach. Reputation is won by an organisation actually handling that problem well. So it is very important there should be transparency, we should know if different identity providers are doing a good job or not. We should know if people are losing data or not, but actually their reputation really depends on how they handle that, how they deal with it, the fact that they reassure you, the fact that they give you redress.
We were nominally talking about access and privacy and there were two real strands that came out of what we were talking about. One is the need for things to be risk based in this space. And the other was around systems, thinking about the issues including considerations of culture and social mores.

The risk-based approach means that it is very important when defining the balance between access and use of information to understand the organisation, to understand the risk, to understand the risk appetite, the residual risk when that appetite has been allowed for and the reputational risk. Some good examples came out right at the beginning of what we were talking about in the health and criminal justice spheres.

We also talked about how to get the right kind of culture so information privacy is respected when handling personal data. We thought the litmus test might be if we agreed the right culture was that if somebody, who is dealing with processing personal data, was asked to do something with it, which they thought wasn’t right, such as going too far or giving it to the wrong person, they would then escalate that issue or be a ‘whistle blower’, if management did nothing about it.

Also when talking about culture we started talking about international issues and of course the difference in culture and approaches to privacy around the world will mean that if you start defining standards about the way to approach these sorts of things, you end up with different interpretations of those standards under the different cultures and therefore you end up with things that may not be acceptable everywhere.

Another thing that we discussed was that the culture required there to be a strong framework of carrots and sticks, sanctions and good things that can happen to you if you do things right, but it also requires constant re-enforcement. The example was given of an organisation where the retention of personal data was signed off on an annual basis, auditing the use of records and an explanation of what they were doing with all their information. The idea was that once it could not be positively stated that data had to be retained it was automatically either removed or archived if it had to be archived.

Table 3 (AS) Focus on registration authorities and ID assurance

The first question was: ‘what is core identity and what attributes make it up?’ There isn’t a specific set. The conclusion we came to is that it is not just one set of data that makes up an identity. For example, if someone goes to court, the judge does not actually care what someone’s name, address or date of birth is, all they care about is that the person standing in front of them is the person that committed the crime and they will put that person in gaol and that person will be tracked through the prison system via an attribute that’s assigned to them. So that person can call themselves what they like. So a core identity is actually made up of lots of different attributes, and it is the whole set of attributes that needs to remain consistent throughout that person’s life and it is not so much about what the attributes are, it is about their consistency and about how they interact as a set.

The second question was: ‘should biometrics be used as part of that identity, if not, what else would offer an immutable link?’ The conclusion here is that there is no one thing that would offer an immutable link. So many things that could be used can be either forged or misused, what you actually need is a set of attributes or set of biometrics, you can’t just use facial recognition, for example.

The third question was: ‘who should have the authority to register a high assurance identity?’ Well, the only people that actually need to are the government. Everybody else tends to rely on the government as it is: when someone applies for a job, when someone tries to open a bank account, you often get asked for a
Aspects of Identity

passport or some other form of ID. It ranges literally from needing to prove identity to the level to work at GCHQ right the way down to a crofter living in Scotland who keeps his money under the pillow.

The level of checks and the level of identity relates to the situation in which it is needed. The only people that need a high level of assurance, the only people that should offer and be able to record to that level is the government and then only where they need to. And we think the debate is still to be had, although we started it, on how much of that can be outsourced, how much the government need to do themselves and how much they should get trusted organisations to do on their behalf and whether the citizens are more willing to trust the government in recording identity or whether they are more willing to trust a private organisation.

Table 4 (PW) Focus on rights and responsibilities of identity providers

One of the first comments was that the various terms – identity provider, consumer, service provider and things like that – are a bit confusing. We looked at the user, what sort of rights and responsibilities they might have and of course one of the user rights is that the data held on them is accurate, but you won’t know that the data is accurate, typically until something goes wrong and there are so many sources of data that it is very difficult for you to be proactive in making sure that it is accurate. This table thought that the Data Protection Act and the regulator may provide some help in relation to this.

One comment was that if you have a single central database and you have a ‘truth’ that is wrong, then it is very difficult to correct that truth because it is only in one place. We felt it came down to the premise that you have got to be able to validate the data, but unfortunately that may very well be where something has gone wrong and that needs to be done at no or low cost. In addition consideration is needed as to whether you are being a persona or a biological person. There were obviously varying levels of how that redress would work. If it was a persona, typically that redress would be done by the service provider or someone in that chain, whereas if it were a biological person there would be a role for a central independent body, possibly an ombudsman.

Thinking of the service provider and indeed other people in the chain other than the user, one of the responsibilities was accurate processing. Accurate processing does include accuracy of data as well. If you could imagine you might have a process where something is being rekeyed, then something can go wrong at that point, so we really do require a responsibility for accurate processing by service providers, identity providers etc.

We also need to think about availability and we had a discussion around 24/7 and realised in fact that while it’s a good thing to aim for, it is actually very expensive and typically won’t be achieved. A number of us on our table have discovered that when you are in a foreign country on a Sunday morning, when you want cash from an ATM, there is no processing, so you need to have availability, but accept that availability is not going to be there continuously.

We have covered redress. I think that one of the last and quite important points that people came up with is again to do with processing the data and it comes down the chain, whether it’s the supplier of a service or whether it’s the identity provider or even further back in the chain that there may be data that is personal data that maybe you don’t wish to be released in a general set. The example that was given was somebody had changed their gender at some point in their life and they would wish to be seen as their new gender and they would not wish a service provider to be able to go beyond a certain point in the data even though the data may very well be stored, so this comes down to controlling access to data and making sure that data can only be accessed by the right people for the right process.
Table 5 (DW) Focus on security versus privacy: the balancing act

The main thing that came out of our discussion was the need to agree scope of what we were talking about. Were we talking about the UK, was it Western Europe or was it worldwide? And how much in this day and age was our data shared abroad as much as within this country?

One of the things that we came up with was the fact that in modern society you are actually pressured into sharing more and more information. If you do, then companies, organisations and governments actually make your life easier for you. We came up with various examples, including supermarkets and people like that. One of the basic principles that has been covered earlier, which I think we all agreed with, was that in principle we only need to give the bare information to whomever wants it and needs it, just the bare information for the particular action that we are providing the information for, but normally the difficulty is who decides exactly what is the bare information and makes sure it’s not re-used?

We came up with a couple of statements off the wall, for instance government IT is definitely not very popular with the general public in this country and another statement that the ID card was going to be cheaper than the passport. One of the things when it came down to national security was very much that it has to be (as indeed it says in the Human Rights Declaration) based on the law, so what national security agencies get up to has to be enshrined in law and indeed people shouldn’t go fishing for information just to see what is there, but rather searches should be focused and authorised.

We then looked at what mechanisms there were for protecting information. One, which we discussed in some detail, was auditing, and accounting goes with that, but one needed changes and flexibility of approach. We also pointed out different types of organisation had different motivations. Banks, for instance, are there to look after the shareholders and get the money passing through. They have different motivation than perhaps governments, who are less motivated by money in the way an organisation that is there to make a profit for the shareholders is. The perception that the security agencies in any country want to put across is that by their actions they are reducing the threat. The big issue I think everybody has, is how can you prove that by having access to personal information you can actually demonstrate you are reducing the threat of such things as terrorism to society?
Annex 3

EuroDIG: The European Dialogue on Internet Governance (Belgrade, May 2011)

This is the official record of the BCS-organised session. A full transcript and a video of the presentation are available at http://www.eurodig.org/eurodig-2011/programme/plenary/identity and on the BCS website at www.bcs.org.

The plenary session on identity, anonymity and privacy was a full session with many questions and discussion points. It was also a slightly different format from the other sessions with the panel asking questions of the audience and engaging in dialogue to solicit input to a range of questions around identity.

For the internet to function and be used to provide services and act as a channel to commerce it is necessary to be able to identify who you are dealing with. But this raises a number of questions. How much personal information is needed, what happens to that personal information once provided and what control does the individual have over that personal information? These were just a few of the critical questions raised.

Louise Bennett (BCS) covered the interaction with a person. It is not necessary in many cases to know exactly who a person is or even who they are in real life. In most situations, such as interacting with an online bank, the thing that is important is to know you are always dealing with the same person: to know the person that created the account and deposited money is the only person who can legitimately withdraw or transfer the money. It is for the bank to know they are dealing with the same person for every interaction.

Andy Smith (BCS) dealt with one of the fundamental problems: the initial registration process. It is clear that for most internet-based interactions the person is remote from the system with which they interact. It is therefore necessary to have a strong registration process that allows the information a person claims is theirs to be corroborated and provenance established. This is to prevent fraud and identity theft, which are fast becoming issues and in some cases barriers to use of the internet.

Peter Wenham (BCS) looked at a practical example of how online services can work in order to minimise the amount of personal data that needs to flow through a single system and how a good trust model can be used to corroborate claims made by a person in order to provide fast and efficient online government services. The challenge, however, once you start linking databases together is to prevent data mining.

The second part of the session looked at the balancing act between privacy and national security.

Bogdan Manolea (APTI – Romania) looked at the basics of data protection as enshrined in EU regulations and Article 5 of the Council of Europe Convention 108. He then covered another aspect of personal data that is becoming more important: the use and collection of biometrics. There is now an ever increasing use and demand by governments to collect and use photograph and fingerprint biometrics, for example in passports. The concerns are that there is little attention to privacy or civil liberties when designing these systems, which could lead to significant risks to individuals.
Ian Fish (BCS) then looked at the specific aspects of consent and the pervasive dissemination of personal information online. He covered the risks of data mining and correlation of personal information to form comprehensive pictures of people and their lives. A possible solution using one-way trust was proposed and then questions posed about how systems can be best engineered to prevent misuse.

Marie Georges (NOOS – France) went into some detail on a very difficult subject, balancing the needs for identity and identification with the basic right of anonymity. Is it possible to be anonymous online? How could this be possible and how can you prevent regulations from undermining rights to privacy and anonymity? A person has to part with personal information if they wish to gain access to a service or perform a transaction, so they should then be fully informed of what happens to their personal information afterwards. If the organisation passes the information on to another organisation, the person should be informed and unless there is a regulatory obligation to pass the information, the person should have to consent to its provision.

The final discussion point came from David Williams (BCS) who looked at the biggest issue most governments face when dealing with people on the internet: balancing national security against privacy. If the weighting is too far towards privacy it can prevent law enforcement and security forces protecting the country and its citizens, but if the weighting swings the other way it can lead to the state having too much information which can be misused or used for unintended purposes.

There was a brief dialogue which covered a number of points from those raised by the speakers. The main one was a question on whether it was possible to have privacy on the internet, to which the response was that once information is on the internet it is there forever. Thus, for most people, it is already too late, as a significant amount of personal information is already there and it would be improbable that it could be removed. It is therefore necessary to educate the ‘Facebook generation’ of the risks they face by being too trusting with what they make available.

At the end a vote was taken on the BCS proposition that biographic and biometric identifiers should be under the control and ownership of individuals not the state or other identity providers. There was unanimous support for this.
Annex 4
UN IGF: Internet Governance Forum
(Nairobi, September 2011)

This is a brief substantive summary and the main points that were raised. The whole transcript along with BCS contributions to other sessions is available at http://www.intgovforum.org/cms/ and on the BCS website at www.bcs.org.

The panel was increased in size before the presentation on the day with Bill Smith from PayPal and Robert Kahn, one of the original designers of ARPANET joining Alun Michael MP, Louise Bennett (BCS) (moderator) and Andy Smith (BCS). Ian Fish (BCS) was the remote moderator, working on communicating with remote participants.

This discussion was about the aspects of identity that affect life online, including identity assurance, privacy and preventing fraud and misuse. It was very good to see so many people attend the session considering the number of alternatives available. There were a large number of participants and this made for an interesting discussion.

Louise Bennett started by giving an introduction about BCS and why the delegation was at IGF speaking about identity. In summary, this was because identity is becoming more and more important in making online activity possible and BCS membership wanted this topic raised. Identity assurance is fundamental to activities such as assured communication, remote access and remote working, provision of government services, banking and commerce.

Without assured identity and proper identity governance models, much of the funding for the internet from business models and commercial endeavours would not be possible.

Three main topics covered were:

• the security versus privacy balance;

• identity governance; and

• trust in remote identities.

Louise started with a description of the problem with access to the internet more and more from mobile devices rather than fixed computers and some 20 per cent of these being lost or stolen each year in the UK, removing any trust you can have in the device for authentication. With the online community connected via more than 25 billion devices to over 2 billion people there is now a massive criminal element at work, thus methods of trust are paramount. The key point was: ‘So it is an inescapable truth that you can neither know who you are communicating with on the internet nor who owns, let alone who is using, the device or the IP address that you are communicating with. However you do need to know both of these things.’
Annex 4 UN IGF: Internet Governance Forum (Nairobi, September 2011)

Andy Smith discussed the balance between security and privacy. The first point he raised was that the balance is often skewed towards privacy, but that it is also the right to privacy and the human rights of all of the victims of cybercrime that are important and that is part of national security and online crime prevention.

The second point was that most trusted credentials issued by government involved a strong background check and an in-person visit. When using these credentials, such as a passport, they are physically checked. However, neither of these processes is appropriate online, where the registration, issuing of credentials and subsequent use of those credentials are remote from the trusting party.

This causes two problems: counterfeit credentials and compromise of credentials through social engineering and technical attacks (hacking). This is more of an issue today because many people have their whole life stored on their computer or even their smartphone: everything needed to steal their identity. The final point was that people think many things on the internet are free, when in fact they pay for them by seeing adverts or providing their personal information, which is either used for targeted marketing or for more nefarious activities.

Alun Michael raised the point that people need to have confidence in the internet and online activities. If this confidence is lost, it would damage the online community. Online is important for government because you can do more and do it more cheaply with a ‘digital by default’ provision of services (using the physical world for exception handling). However, he pointed out there is growing evidence that a significant portion of the UK population would not go online even if you gave them a computer and broadband connection and this is likely to be similar in other countries. This is to some extent a question of fear.

He made the point that he and other legislators were very reluctant to legislate in this area unless they had to and that the impact of legislation on the internet was often unpredictable and ended up having undesired consequences and could be completely out of date by the time it became law. This makes it all the more important that what we are doing is making clear what the principles and responsibilities are rather than trying to put in place regulations and legislation that is technology specific or specific to a particular point in the development of these ways of using communications. There is no central control of the internet, which is one of the reasons IGF is so important. He raised the issue of who would be appropriate to govern identity assurance on the internet and how some governance models would work. Is it a question of control or one of standards?

The following discussions raised many good points. One, raised by Bill Smith, is that PayPal find three things of key importance now: these are anonymity, pseudo-anonymity and attribution. They believe in using attribution in various levels as and when necessary. He made the point: ‘In the United States that was a very important part of the founding of our country, the ability to speak anonymously and it is embedded in our Constitution.’

The point about liability in business was made because this is very important. Often it is not necessary to have a detailed identity or even prove an identity, only to ensure that the person that was registered is the same person performing the transactions in the future. This is especially important for credit card and online banking. There are, however, legal requirements for knowing who customers are and being able to trace transactions to individuals when necessary. This means the registration needs to be strong, but the use of credentials do not need to reveal details about the identity.

Bill Smith also detailed the distinction between identity and authorisation. This led to a debate about the attributes and the different requirements needed for proving identity, performing an authentication and authorising an action. This included a discussion on the need for different levels of authentication for different types of transaction authorisation. You would not transfer someone’s life savings based on a username and password. Ian Fish brought in the first question from a remote participant who raised the difference between the European concept of privacy and the US principle of openness. This raised a
number of responses, which covered this as an example of the need for international debate and the need for different philosophies to operate together and interact. Again there is a balancing act between privacy and openness.

The discussion turned to misuse of information access and the ability to identify individuals, especially by oppressive governments, which means that online there needs to be the ability for the same individual to be anonymous for expressing opinions and fully identifiable for online banking and commerce. Separating the two can be very difficult.

Robert Kahn made a number of points about the changing technology, especially around the use of identifiers for things rather than people, such as IP addresses and how even this is changing. You can use different systems, but there needs to be more standardisation to make systems compatible and allow them to work together. Such examples are public key infrastructure (PKI), where a private key can be used as a credential for a person, token or device. This is currently the most effective credential and as long as the issuance process and protection of the credential are effective it can be used to underpin various identity systems.

One participant made a clear statement about the nightmare scenario: ‘The idea when there will be introduced global authority for identities on the internet, where every person will be required to have one identity, because it will make us traceable and accountable on the internet, because we need to be anonymous, but almost all services will be oriented only on citizens with one identity.’

Andy Smith raised the point that it’s only really governments that need to know the true root identity of a person and that is mainly for national security and quite often that’s not even for criminal prosecution. If you commit a crime, what the law enforcement and judicial process needs to know is that the person that committed the crime is the person they have put in prison. They don’t even need to know you are who you claim to be. They don’t care what you are called, but they care the person who committed the crime is the person who is punished.

Various people made the point that there are a lot of laws around money laundering, around criminal fraud etc., that require a level of knowledge of identity for reporting. However, quite often a minimum of personal data can be used as long as the organisation that’s actually performing the financial transactions has access to more information should they need it. The transactions themselves can use zero knowledge, proof of knowledge, one-way trust and other methods in the transactions. So the identities themselves can be pseudonymous or linked to a root identity.

Andy Smith raised another point on compatibility and interaction. The UK Government is looking at how you can put authentication systems in place with identity credential conversion. So rather than trying to get everyone to use the same credentials or the same authentication mechanisms, actually putting in converters so someone can use PKI, someone can use SAML. You have got devices that can accept the trust from one authentication system and pass it on to another authentication system and this will hopefully allow different systems to interact with each other and actually try and get some of these commercial models more stable. The conversation then turned to the research and policy perspectives around seeing if two parties can have these transactions directly and be able to authenticate when there is no central party that is guaranteeing identity. eBay was used as an example of this where reputation was used as a form of trust.

The discussion then turned to use of biometrics, and both the use of biometrics online and the ability to counterfeit and fraudulently use them. This was especially interesting with facial recognition, where web-cams and even mobile phone cameras can be used. For example, there is the potential from systems that would use facial recognition as a way of encrypting or decrypting files on your computer to improve privacy but increase authentication security. Unless your face is in front of the computer, then the file would not be decrypted. This is something that is already being trialled in UK hospitals. Louise Bennett stated, ‘I think it is a very exciting way of doing it. I use my biometric to log on to my machine. It seems much safer than
anything else and it is much quicker.' Andy Smith mentioned that this is also being used for automated gates at passport control right across Europe now.

If you can tie a person’s identity to the individual using immutable credentials like biometrics, then it does make things a lot better because it can prevent people stealing identities, or at least it makes it a lot harder to steal identities because you have to replicate whichever biometrics you use.

Another remote participant was curious, asking if the USA and NSTC had come up and how they might be shaping global governance. This was discussed and the conclusion was that it had not really had an impact yet.

The discussion returned to biometrics and the worry that biometrics could be stolen and misused. The point was made that if you are doing biometrics properly, this is not really a concern because you do not use the source biometrics in the credential system and if you do, they are backed up with other measures such as encryption and digital signatures, so cannot be counterfeited or forged. European governments are putting in a system with BAC and EAC for use with passports addressing these problems.

The final discussion concluded that when information is required, for authentication and authorisation, it should be kept to a minimum and what is appropriate for the transaction given the context in which it is happening.

Louise Bennett finished the session with two questions:

‘We had quite a lot of talk about whether people should have one ID or many IDs. Could everyone who thinks people on the internet should have one ID put up their hand?’ No hands were raised. ‘Should people be allowed to have many IDs?’ Everyone raised their hands. ‘That’s pretty conclusive, which is quite helpful. Consensus, yes.’

‘The second point that I’d just like to ask you is: do people think that the way to deal with remote IDs is through trusted third parties? Do they think that is a route that is worth pursuing? And again those who think that is a route that’s worth pursuing in this area could you put up your hands?’ A mixed response. The consensus was that trusted third parties had a role to play in some contexts.

Conclusions and further comments

There is a balancing act between security and privacy and the balance needs to be moved nearer security in some countries, mainly Europe, and nearer privacy in others, such as some countries in the Middle East.

There is another balance between openness and privacy where sharing of information is important in some contexts and privacy is not a fundamental right, but in other contexts privacy is a right and should be respected.

The rights of victims of cybercrime should also be taken into account when talking about rights and privacy online.

There needs to be more standardisation of identity systems and better processes for registering people into identity management systems online. Credentials need to be secure with private keys and biometrics being two strong credentials, but the issuance processes need to be improved to reduce identity theft and fraud.

Only governments really need to know the true root identity. For most online activity organisations just need to know that they are dealing with the same person at every interaction, or that the individual has the ability
Aspects of Identity

to deliver their part of the bargain (money or goods). There are however some legal requirements to be able
to link a person back to an established root identity, this is usually done via a strong government-issued
credential such as a passport.

There is a lot of work to do on identity governance, and organisations such as IGF and the UN will play a part
in this, but a centralised governance model is inappropriate for identity on the internet.
Annex 5
Parliament and Internet Conference
(October 2011)

This is the summary of IGF impressions related to internet governance by Louise Bennett, published in Messages from Nairobi presented at the Parliament and Internet Conference.

My main take-away impressions of the sixth IGF were as follows.

That the European view, as expressed by the Council of Europe via EuroDIG, that puts human rights and net neutrality as absolutes at the top of the agenda, without due consideration of the proportionality between security and privacy was not a governance model accepted widely. The reality is that users expect their data to retain domestic levels of protection (whatever these may be) whatever jurisdiction they are in on the internet. Common principles and compromises are needed, but these will be very hard to achieve. It is important to consider processes and liabilities. For this reason more delegates from both the financial and legal sectors need to attend IGF.

For individual users the internet is ‘experiential’. Trust increases with use and depends on the national and individual starting points. In developing countries, trust rested largely with major companies, such as Google, Microsoft and Facebook. In relation to privacy rights, it was widely accepted that there needed to be an internationally agreed definition of what comprises ‘sensitive personal data’.

Only a small number of principles are key to internet governance: open architecture; multi-national, multi-stakeholder dialogue to develop good governance and an understanding of conceptual meta-level approaches to complex networking with the adoption of interoperability standards.

Governments need to have a policy to ensure their citizens have access to a safe and secure internet, to encourage social interaction, access to content and development. Outside the EU, our data protection laws are seen as a protectionist device and not a strongly held principle, because the key for users in developing countries is that the internet is cheap and flexible.

There was also resentment about blocking of certain country domain names on fraud grounds. Domain name system filtering and blocking was seen by many as an excessive focus on illegal online content that impeded creativity, fostered criminal activity and damaged the internet. By attacking the content via ISP addresses, law enforcement agencies were blocking consumption, driving services underground and bringing only short-term relief because the content just reappeared elsewhere. If content was illegal, law enforcement should find and prosecute the perpetrators.

Ways forward on internet governance were suggested via: CSR reporting in company accounts; suitable international conventions that countries could sign up to; consumer protection agencies, because most
countries had these and many countries already had bilateral and multilateral agreements across borders that could be developed for internet trading.

The sixth IGF saw the resurrection of a Dynamic Coalition for The Internet of Things to develop understanding of governance issues (if they differ from current issues) and take them forward. There is an opportunity for the UK and BCS to be influential from an early stage in this developing global initiative.
This is a brief substantive summary of the main talks at the thought leadership seminar produced by EEMA.

John Doody, of Interlocutor Services Ltd, welcomed delegates to this thought-leading seminar on eID on behalf of BCS and EEMA, stressing the need for initiatives such as this to bring experts together and find solutions.

Talking of his own experience, he confessed to being a computer ‘geek’, doing everything online, from banking, tax and VAT, corporation tax, vehicle tax, booking holidays and flights, buying from Amazon and train tickets etc. And for each transaction he needs to provide an individual password and other identity attributes to be trusted. Colonel Doody also confessed to being a ‘card freak’, possessing hundreds of cards for garages, shops and a host of other organisations with which he does business.

However, he viewed the utopian situation as one whereby he would have to use just one card for all online transactions. The great challenge is not the technology: it is in place. The challenge is one of privacy and personal issues. As the use of the internet and internet transactions is rising exponentially, so does the need for practical solutions to carry out business transactions securely.

Jim Norton, BCS President, welcomed the delegates and described the vision and objectives that had migrated from purely membership services to public services. He continued by outlining the various work groups of BCS and their activities.

Roger Dean, EEMA Executive Director, opened the proceedings by providing an overview of EEMA. As he said, it is a platform for Europe that provides a networking forum for professionals in the fields of identity, identity management and security. Roger’s involvement in the industry started when he introduced the first commercial email platform in the UK, France and Switzerland. In those days email was used much less frequently than today, and machines could be turned off for hours before anyone noticed. That situation has changed dramatically, but the two main issues, which prevailed when EEMA was inaugurated 24 years ago, and which form the basis of EEMA’s work today, have not: security and interoperability. Today, however, the interoperability debate is more to do with identity and attributes etc., rather than X.400, X.500 as it was in the 1980s.

EEMA’s work involves many different areas: it provides an online bulletin for its members on a bimonthly basis; reports on events such as this; articles; an online discussion forum for IT professionals; and a number of important, pan-European events such as:

• a Regional Interest Group meeting being supported by KPMG in March;
• an interoperability conference in Switzerland, also in March;
Aspects of Identity

• its Annual Conference, to be held in Paris in June; and

• ISSE, the annual security conference, to be held in Brussels in November.

EEMA also works on projects inaugurated by the European Commission. For example:

• STORK, which has been running for three years, and which has launched five successful pilots. It is now moving into its second phase: STORK 2.

• ETICA, a project which looks at ethics in regard to technologies such as social networking.

• SSEDIC, which exists to advise the EC on a strategy for pan-European identity.

Louise Bennett, Chair of BCS IAWG, presented the findings from three workshops on identity assurance run by BCS. The first was at Infosec in London, and most of the delegates came from a technical background. The majority understood eID assurance and felt that security trumped privacy: a view strongly aligned with that of BCS. However, at the EuroDIG conference in May, many delegates were human rights/privacy advocates and came from a non-technical background. They felt that privacy and anonymity trumped everything else. At a third, the UN Internet Governance Forum (IGF) in Nairobi, yet a different viewpoint was predominant. The delegates were mainly government officials, law enforcement and criminal justice agencies, while financial organisations and entrepreneurs were underrepresented. The majority view was that everything should be done to keep citizens safe and promote economic development.

Some of the results of the workshops demonstrated that:

• for many users, particularly at the IGF where many delegates came from developing countries, the internet is ‘experiential’, so that trust in identity over the internet increases with use, and differs widely according to culture;

• many users in the developing world trust big companies, such as Microsoft or Google, but not necessarily their governments, and were not concerned about privacy. If cost could be kept low through data mining, then that was more important.

For ecommerce, Louise stressed that the important thing is to track down and prosecute criminals, but that it is necessary to balance the rights of users against the rights of victims. In terms of who or what needs an identifier, she explained in detail the different requirements for applications, things and people, along with different levels of risk, the flow of liability and what needs to be private versus what needs to be public.

At the IGF, many saw filtering and blocking as an excessive focus on illegal online content which would impede creativity and damage the internet. Many felt that law enforcement agencies should track down the criminals rather than block the site.

While many delegates at the IGF felt that IPv6 would provide everyone with the ability to have just one unique identifier for the internet, all agreed that multiple identities were desirable. In repressive regimes this was seen as particularly important, so that individuals may be fully identifiable for certain transactions, but remain anonymous when, for example, expressing an opinion.

There was also a strong feeling at the workshops that there was a need to define what sensitive, personal information is. However, in Louise’s view this is almost impossible to achieve on a global basis because it depends upon culture and context.
Louise concluded that there are four broad principals essential to ensure good internet governance: open architecture; multi-national stakeholder dialogue; a meta-level approach to complex networking; and the adoption of interoperability standards.

Frank Leyman, of Fedict, discussed the Belgian experience in implementing egovernment. As someone with a marketing background, he started by explaining that the first job was to analyse what would motivate citizens to take part in egovernment: the drivers. These were defined as:

- efficiency when dealing with the government;
- speed of execution;
- transparency – the citizen wants to know what the government is doing with his/her data;
- cost – as low as possible.

Civil servants also want these four requirements. However, it is also necessary to look at different types of citizens. For example, the younger generation all have mobile phones, and even if youngsters are in the same room they are likely to send each other text messages. The question then arises: how can egovernment adapt to these citizens’ needs? If you look at the working population, they simply want to be able to work anytime, anywhere with no communication problems; and the last group, the elderly, wants to take part but may struggle with the technology. While the technology necessary is there, it is important to be able to communicate with the different groups.

Frank also stressed the importance of having not only a good front office, but also a good back office, and the Belgian Government spent four to five years reorganising its back office. The identity card was the next step.

In Belgium, the national identity card is mandatory from the age of 12. It holds the minimum amount of data necessary: name, date of birth, gender and some numbers. It contains two certificates, one for authentication and one for digital signatures. The citizen’s official address is on the chip. There are three variants: children, adults and foreign residents. The Government did not concentrate on building applications, but rather focused on technology, thereby allowing the private sector to create applications. Frank outlined some of the many applications, from ordering documents to gaining access to a swimming pool, discos and reporting minor crime.

Education was a problem, and so the website has a Q&A section on it. In addition 300,000 card readers were distributed to citizens to enable them to use the cards. In terms of transparency, any citizen can view online any official who has accessed their data. To enable municipalities to build applications easily, off-the-shelf modules have been built that can be copied and pasted. Current initiatives include rebuilding identity and access management, trying to make services independent of hardware and extending the back office both to regions and communities, and to other countries.

David Rennie, of the UK Cabinet Office, discussed the problems of accessing internet-based services, the need for identity assurance and the proposed model for the UK, which he described as customer-centric: customers will be able to choose their identity provider(s) and a hub will connect them. Logically, it should be a single hub, but for security reasons a distributed model is preferable. The hub ensures that identity policies are adhered to and passes information onto the service provider that can then make its own decision based on risk.

In terms of validation services, the public sector holds much information that could be used to validate paper-based identity documents digitally. Thus, if one wanted to use a passport to prove identity, the identity provider should be able to validate that the information on it is correct. However, the identity provider should not be able to capture data about the passport. In the model proposed the passport owner will, for
example, be able to obtain validation from the passport office and pass that back to the identity provider. A key feature of the design is privacy, so that the customer controls his/her own data and how to share it, and it is that which makes the scheme complex.

There are several security benefits associated with the model: validation services ensure that documents are not forgeries or good copies; a mechanism for relying parties to feed into the ecosystem when they catch a fraudster, such that the identity can be ‘turned off’; and a transaction monitoring system built into the hub. The UK Government will shortly be releasing a draft document outlining new identity standards, but recognises that standards change, such that it will need to be updated constantly.

Tom Ilube, of Callcredit Information Group, discussed an initiative called Noddle. He had been particularly interested in discovering what would make consumers engage in their own electronic identity. Traditionally in the UK, most consumers don’t care about electronic identity; it is only some sectors, such as the media, that focus on it. When identity theft happens in the UK, most just shrug their shoulders; and regulation produces reluctant compliance rather than engagement. In terms of incentives, Tom mentioned financial gain as an obvious one, but strangely, simple curiosity is another.

Callcredit has 45 million credit reports, and Tom got the board to agree to make them freely available online, for life. The trial initiative was announced in June 2011 to see what kind of consumers would want to take part. The results showed that 70 per cent of those who accessed their credit reports were male and between 25–40 years of age. The younger and older segments were not as interested. Tom estimates that within 2–3 years, he could have an online community of 2–4 million consumers, all highly verified and authenticated, making him part of the identity landscape.

David Birch, of Consult Hyperion, looked at how eID might work with the financial services sector. He started by looking at some of the current problems, such as dongles that will not work within different branches of the same organisation; the necessity for different passwords according to different organisations’ requirements; the possibility of hackers gaining access to many different accounts if only one password is used; and forgetting passwords.

One of the main problems he saw was that the UK has no particular policy regarding identity, and so the technologists do not know what is required of them. The Centre for the Study of Financial Innovation has looked at various models, such as the Scandinavian model where the bank ID is at the heart of the interaction. This model has migrated well into the mobile world, but is somewhat dependent on specific conditions, for example, Scandinavia has only a small number of banks that work well together. This is a zero liability model. In Southern Europe people use the government ID to log into the bank. The US model is different again. The government issues the framework and standards for identity and the private sector provides the identity. Both public and private sectors provide the attributes.

In terms of the UK, David felt that the banks should present a more consolidated approach.

He outlined some principles for etransactions:

• Industry and not sector standards.
• Multiple identities as a legitimate right with privacy enhancing technologies.
• Greater use of the mobile phone, which everyone possesses.

Finally he noted that banks could fulfil the role of identity providers. Attribute provision could also be a good role for them because they know a lot about their customers.
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 e-commerce. 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 e-commerce and e-government to thrive. The Identity Assurance Working Group was therefore established to examine the governance and other issues surrounding identity assurance on the internet.

The group ran a series of workshops at UK, European and UN events to collect national and international views and explore the key underpinnings of identity assurance principles, rights and responsibilities, including information rights and privacy, in an interactive and multi-stakeholder format. The collective results are presented here, together with the critical issues on which the group will focus its continued dialogue throughout 2012.