bcs
The Chartered Institute for IT

Enabling the
information society

Aspects of Identity Yearbook 2014-15

BCS Identity Assurance Working Group

Introduction and Overview

Over the last four years the Identity Assurance Working Group (IAWG)[1] has been examining the governance and other issues surrounding identity assurance on the internet. The 2014/15 Yearbook builds on the previous work. Readers can find the annual yearbooks and follow the development of thinking around the topic at http://policy.bcs.org/content/identity-assurance-working-group. The main findings and conclusions are given below. The individual workshops and talks given by the IAWG members in 2014 can be found at http://policy.bcs.org/content/reports-research-papers-and-presentations.

1. The Role That Identity Management Plays In Trust On The Internet

Transactional security is vital for Internet Commerce. Effective policing and protection of citizens' rights and identities are vital for citizen trust in the Internet. Whilst the ability to perform financial transactions anonymously is needed in some specific circumstances, it is very hard to base general solutions on this principle. In the meantime, wider benefits would be obtained by finding ways to make it easier for strangers in a transaction to identify each other to the extent necessary for that transaction.

It would be helpful to refocus the Human Rights debate, which has become polarised, onto Digital Trust. Standards for digital identity and digital payments are needed, particularly in peer-to-peer payments. The UK Government should incentivise citizens to embrace the roll out of GOV.UK Verify and support the open standards for online identity and payments being developed by the World Wide Web consortium (W3C).

People in many developing countries regard the EU Human Rights Act and the legislation and regulation that flows from it, as a protectionist policy not a statement of principles. If the UK is to gain global acceptance for UK views on Digital Trust, it would be better to refer to the International Covenant on Civil and Political Rights (ICCPR), which has been signed by more countries than any other, rather than the UK/EU Human Rights Acts.

Education rather than legislation is critical in developing trust in using online channels. There are some international cybersecurity messages, based on extensive research, that the UK should consider adopting, such as: "Stop, Think, Connect" and "Safer for me, Safer for you".

2. Different Routes To Identity Assertion

Real transparency on data collected by business/governments and robust oversight mechanisms are needed in connection with digital identity and digital trust. In some countries (e.g. most of the EU) identity assertion is only done by central government. In others (e.g. the UK and USA) identity assertion is carried out by a range of private sector companies by matching source data from both government and the private sector.

The EU is seeking to achieve interoperability between these disparate national schemes for member states through a new regulation on e-Trust. The BCS has concerns that this regulation, far from encouraging the expansion and reliability of cross-border e-commerce, will instead increase costs, inhibit growth and not only obstruct access to global e-services by EU citizens and businesses, but also restrict the free movement of services within the internal market.

In the UK and across the world we are seeing the increasing use of private sector electronic identification for access to public sector services. The EU proposals will introduce a blanket burden of both proof and liability on providers, a disproportionate supervision scheme, and unnecessary regulatory constraints which will inhibit the establishment of new trust service businesses in the EU. They would give Governments vaguely defined powers to interfere in private trust services and grant further powers to the EU Commission outside of Parliamentary approval, which may contravene the Lisbon Treaty. The regulation should change emphasis. It should affirm the relevant international (ISO) and European (CEN-CENELEC-ETSI) standards for governments, citizens and businesses to adopt as appropriate as this rapidly changing technology evolves, rather than try to implement central control through legislation.

[1] IAWG Members 2014 – L Bennett (Chair), J Bullard, L Coles-Kemp, R Dean, I Fish, G Rosner, A Smith, T Stevens, M StJohn-Green, P Wenham, A White, D Williams

3. The Use Of Big Data Including Personal Data In Asserting Identity And Tensions Between Privacy, Anonymity, Traceability And Security

BCS believes that ethical use of big data will support the growth of the digital economy and, conversely, misuse could seriously damage trust in the internet.

A discussion on the ethical issues on "big data" exploitation by governments and businesses (both active and passive data) is needed. There are obvious benefits that can be secured in, for example, health and social care, disaster management and relief, and solving or discouraging crime. However, all of these advantages can be lost if misuse of big data results in loss of trust in the internet because of abuse of the power it is capable of conferring on commerce and government.

Identity, discovered through data aggregation, is already used as a form of currency on the Internet, with people providing personal information in order to gain free or low cost services in return. This allows the "payment" for those services to come from targeted marketing and other sources. (See also

http://policy.bcs.org/position_statements/online-anonymity)

There is growing global awareness that government surveillance, commercial abuses of privacy (particularly tracking GPS and surveillance connected with Smart devices in everyday objects, such as cars and TVs) and sloppy handling in the public and private sectors via the collection and analysis of personal data have got to be tackled. It is Orwellian double-think for Governments or corporations to say that privacy means keeping information between me and you, when individuals think privacy means keeping information to themselves.

A practical way forward would be to focus on what realistic privacy rights people want and what harms need to be stopped. It should be accepted that in a digital world where products are connected to the internet and in "a sharing economy", the concept of "informed consent" is a straightjacket that is increasingly difficult to implement provably and consistently. The UK Government should lead thinking on this complex topic and move to the principle of practical privacy by default, not tracking by default.

The BCS position is to support an ethical approach to the use of big data by proselytising the need for transparency, control and consent in situations where the data identifies individual people (which is increasingly the case). All users of big data should be encouraged and helped to understand the limitations, including the risk of de-anonymisation, of the products. To support this research effort is needed and, crucially, education of citizens on the benefits and perils of big data is essential

(http://policy.bcs.org/position_statements/ethical-use-big-data).

For users of big data it should be an offence to act inappropriately when you have re-identified someone. The act of re-identifying someone, being an inevitable consequence of handling big data, should not itself be an offence. Offences and sanctions for acting inappropriately should be on a par with those relating to data protection.

It is now widely acknowledged that information on the Internet is discoverable by anyone determined to do so. Absolute privacy and anonymity online are chimeras. However, people do need to have the means of ensuring security for their online identities that is commensurate with the contexts of different online interactions.

There is still a lot of work to do to understand the different drivers for security, privacy and anonymity, including how they pull against each other or overlap. In particular, tensions exist between those who advocate the enforcement of strong, unique identity to aid National Security and those who oppose it on the grounds that anonymity protects the weak with good intent.

There will never be global agreement on proportionality, but the IAWG is attempting to work towards global understanding of different perspectives and the ability to accommodate most of them.

4. Levels Of Identity Assurance Needed For Financial Transactions

There is growing awareness that internet enabled commerce which invariably ends in a financial transaction (i.e. a payment) represents a key element of global growth. .

It is also worth noting that the threshold of painful loss for an individual is far lower than the threshold above which any law enforcement agency is prepared to investigate. This means that redress for the individual in online transactions that go wrong needs to be managed upfront as is the case with the Card networks.

BCS consider that the focus for all transactions involving online payments needs to be on building trust between the parties. For trust to be durable and effective, there needs to be a regulated and enforceable framework to ensure that roles & responsibilities, liabilities & obligations are clear and the means of redress are effective. Lawmakers within a nation state context should steer clear of attempting to be overly specific. Instead, in a global context, they should ensure that the Law of Contract between parties can be freely adopted.

In most situations both individuals and businesses need to be identifiable and not anonymous when making on line transactions involving payments.

Three levels of transaction need to be considered, high, medium and low. Banks have provided usable solutions to the high and medium levels throughout the developed world and globally for commerce between major companies and via credit cards for individuals. It is low level transactions peer to peer and with small businesses that need to be the focus of any new open web standards.

Any e-identity technology standard on the Internet must also allow for multiple identities. Organisations and individuals need to be able to assert their identities from many places and devices. All the surveys and research show that individuals want to be able to use multiple identities for different roles/aspects of their daily lives. It is also necessary to accept that you cannot provide 100% security. You have to balance usability with security and consider the risks involved in every type of transaction. In online transactions, as in the paper world, there is invariably a trusted third party, ideally a regulated financial institution (i.e. a bank) or perhaps like Alipay standing in escrow for Alibaba transactions, or indeed PayPal acting as a trusted intermediary.

UK should propose a workable approach to the need for the jurisdiction applicable to every financial transaction conducted by a member of public in the UK to be clear and unambiguous. UK should press for international legislation on criminality on the Internet with much faster responses to Mutual Legal Assistance Treaties (MLAT) requests. (At present these take months or even years to enact).

In the physical world most of us know how to get redress if we are cheated. We know the consumer rights we have in our home country. In the online world we can face much more uncertainty, particularly when our transactions cross borders and jurisdictions. Mutually agreed operating processes (a blend of Policy Legal Operational and Technological Standards) are needed to reduce that uncertainty.

Conclusions and Recommendations

Trust is the key driver for internet usage and particularly for commerce on the internet. Trust can be fostered by:

- Effective law enforcement in cyberspace, including international co-operation.
- Identity mechanisms that are sufficient for the transaction and reliable.
- Clarity on contractual liabilities and redress for internet transactions.
- Legislation and regulation that is proportionate and understandable.

To advance these ideals, BCS advocates international approaches to identity management, law enforcement and transaction management on the internet that are specific to the issues, clear, unambiguous and in step with the speed of development. The role of education and awareness of all internet users is key; regulation and legislation should be as minimal as possible. Internet security is only likely to be improved significantly if the majority of actors voluntarily agree to some norms, as has already happened with criminal child online exploitation.

Looking to the future we believe that the ethical use of big data and the associated local and global linking of myriad data sources (the so called internet of things) into critical infrastructures will become a major issue but that these are susceptible to the same types of approach outlined above.