Anonymity on the internet background paper

Introduction

In the virtual world we may want to know who we are dealing with, but with varying levels of certainty according to the context of our interactions. In some interactions anonymity is fine in others it is not.

Anonymity on the Internet can be an emotive and misunderstood issue, so it is important to define the terms we are using.

The heart of the debate about anonymity concerns the potential for abuse by the anonymous and erosion of privacy for those who are not anonymous. There is a significant difference between privacy and anonymity.

On the internet, anonymity is the ability to perform actions without them being traced to the person. This ensures both that individuals can enjoy the right to free speech without fear of repercussions; but also that people cannot easily be identified and held accountable for their actions.

Privacy is what allows people to keep what they know to themselves. Privacy is the ability to provide personal information only to those who a person chooses to provide the information to of their own free will, or to those entitled to it by law. Privacy protects people's rights, and does not, per se, damage national security and law enforcement (although it can make them harder to achieve). However, anonymity can cause damage. Anonymity is not necessary for privacy, but is often misinterpreted as being synonymous with privacy.

A final related concept is secrecy. This again is not the same as privacy. Secrecy is about what is known, but not to everyone. Secrecy is what the intelligence services strive for. All three concepts, anonymity, privacy and secrecy are underpinned by appropriate security.

Devices not users are directly connected to the Internet

It is important to remember that devices and things are directly linked to the internet not the users of the devices (neither individuals nor organisations). Identifiers are needed for all of these devices and things and also for other resources such as applications. It is critical to have trustworthy identifiers associated with devices and things in order to know you are getting the right data from the right place (the right on-line 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).

So, since people and organisations are not directly attached to the Internet how can you know who is using or controlling the thing that is attached? You can just assume that your friend is texting you from his phone, but what if it has been stolen or someone has borrowed it? The same applies to a PC, not just in an internet cafe, but also in your home, where other members of your family may share it, or in a library. It applies when a device has been compromised by a criminal or a malicious individual.

So identity on the internet is often about knowing who is using the thing. How certain do you need to be that a specific individual or organisation is using a particular device?
Identity and Anonymity on the Internet

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

Everyone: individuals, business and governments also need to understand that anonymity and traceability are different issues. On the Internet, anonymity is the ability to perform actions without them being traced to the person. This ensures both that individuals can have the right to free speech without fear of repercussions; but also means that people cannot easily be identified and held accountable for their actions. Tracing those apparently “anonymous” postings is known as traceability. Traceability at its most benign is a protective law enforcement requirement. In Western democratic societies it is most often used in a reactive manner where there is good legal cause.

The Childnet Youth IGF Group defines anonymity as “the ability to interact online without being compelled to reveal who you are”. There are strong calls from most stakeholders to ensure that anonymity on the internet is retained. For example, 86 per cent of young people who responded to the Youth IGF Project “Global Perspectives on online anonymity” supported this call. The BCS Identity Assurance Working Group (IAWG) has also had a similar response in all their workshops over the last three years.

However, it is important to realise that true anonymity on the internet is not achievable - it is always possible to trace at a minimum the IP address people are using, and then it is usually possible, with sufficient resources, to determine who they are via access to multiple data sets. True anonymity is, therefore, extremely difficult to achieve. People also worry that anonymity can be misused, for example for criminal activities, cyber-bullying and so on. In addition, some people quote examples where they say anonymity is important where people are not seeking complete anonymity, but want to reveal themselves only to a trusted group. For example Arab Spring members; while they wished to remain untraceable to the authorities, did not want to be anonymous to other members of the movement. If they were truly anonymous how could the other members trust them?

In August 2012, in the South Korean Constitutional Court, OpenNet Korea, the BCS’ joint workshop organisers at the UN IGF 2013, won their case against the South Korean Government’s 2007 regulatory regime that required “mandatory verification of user identity” in online services. The regulation was declared unconstitutional.

While freedom of expression allows individuals to say things that some people might find offensive, criminal activity should always be prosecuted. It is the failure to prosecute those behaving criminally on the internet that has allowed “bad actors” to dominate many debates on the topic of anonymity. To do this effectively, the definitions of criminal behaviour and the rules of social behaviour need to be agreed internationally, together with enforcement mechanisms.

It is also important to recognise that not every internet interaction should have the privilege of anonymity. The context of such interactions is important; for example, some private

1 Global Perspectives on online anonymity = October 2013 – Youth IGF Project – Childnet International
interactions, such as those to financial institutions, may well need to identify the person making the interaction positively. Other interactions, such as email, will at least need to associate the interaction with a pseudonym, which may actually be operated by a single person or a connected group.

There is still an ongoing discussion as to the exact contexts in which it is acceptable to be anonymous as well as to the meaning of the access afforded to law enforcement agencies under the Human Rights Act and various national legislations. In this discussion, it is important to understand not only who is seeking anonymity, but also who they are seeking anonymity from and the reason why.

In connection with all the issues associated with online identity there is a growing need for widespread public education about safe use of the Internet. This is a key requirement for the Internet to flourish and to ensure that all nations, businesses and individuals get economic benefits from an increasingly online world.

A final point that is particularly important for legislators to take on board is that identity solutions need to be designed for tomorrow’s business models, not (just) for today’s. Legislators have got to be much more agile than they are now. It reinforces the view that grand schemes are not going to provide the answer, because changes and the growth of new solutions for specific problems are happening too fast. It is important that legislators solve practical real world problems that individuals and businesses face, pragmatically, as those problems arise.

In order to achieve this it is necessary to have robust identification of businesses and individuals for all financial and contractual transactions. The EU said this in its cyber security strategy: “Secure, stable and resilient networks form the basis of a trusted and flourishing Internet economy”.

On the negative side criminals tend to follow the money. With more financial transactions and purchases moving online, the criminal elements are following, making identity assurance all the more important.

Identifying individuals through Chains of Trust

When we identify someone, we sometimes want to establish that they are a unique biological being as recorded on their birth certificate (this is known as the root identity) and sometimes that they are the same “persona” who did something at a different time. So it is necessary to think about when you want to know a person is a specific biological individual and when do you merely need to know that they are the same avatar or person you interacted with yesterday.

You need to know a biological identity when you are issuing a passport, but only the avatar when you engage with someone in an online game. Even if you want to withdraw money from the bank account you opened last week, the bank only really needs to know the persona you are using. This is because in a banking transaction the key thing that matters from a bank and customer perspective, as opposed to a legal “know your customer” perspective, is that you are the same persona who opened the account and deposited the money.

Being certain of a person’s biological identity involves a chain of trust.

A chain of trust is the classic passport model where you can match the credential for the identity to the biological person. To demonstrate this online typically the individual uses a token – “What you have”, this is linked to some biometric “What you are” if you want a high
level of security. This may be picture of your face, a fingerprint, voice print or even in New Zealand your DNA. It is also likely to be linked to some attribute about yourself “What you know” – your date of birth, school, mother’s maiden name for interactions needing a lesser degree of certainty.

It is these attributes, otherwise known as personal data, that can get people really worried, especially if they are keen on privacy. This is because a common way of identifying people online is through a network of attributes.

**Identifying individuals through Network of attributes**

A network of attributes provides an authorisation model using multiple low assurance sources of identity and associated attributes. Whether you identify someone through a chain of trust or a network of attributes is all a matter of the risks you and the other party are prepared to take in the context of the transaction you are involved in.

One of the real problems we have online is identity discovery through data aggregation. When we think about privacy, particularly in relation to commercialisation of the internet, and Government surveillance and data collection, this is what people really object to. The analysis of “Big Data”, without either their knowledge or permission (see background paper on the ethics of Big Data).

Yet those same people may be happy to build up a reputation score on auction sites like e-bay to ensure they have a reputation as a trustworthy person to do electronic business with, irrespective of whether they are using their real root identity or an “anonymous” e-bay identity. How each individual feels about different uses of data aggregated and associated with their identities is highly personal and highly contextual.

In UK law, we can use multiple identities (which may not be allowed in other countries) and there is no problem with us doing this provided we are not intending to deceive or defraud others.

However, once big data analysis enables identity discovery through attributes, can there ever be certainty of anonymity or indeed privacy? This leads many people to use multiple identities on the internet to frustrate data aggregation about themselves.

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

**Security versus Privacy & Anonymity**

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

Many of the arguments raised against privacy advocates on the internet concern the inability to hold people accountable for their actions. These concerns normally stem from anonymity rather than privacy. Even in EU data protection legislation, there are clauses for law
enforcement and national security that take precedence over privacy and this reduces the impact of data protection on true national security objectives.

An anonymous person committing fraud, bullying, a terrorist or serious criminal act over the Internet is very difficult to catch and hold accountable for their actions. However, anonymity is reasonable in connection with many transactions, interactions or conversations. It is also needed where there are fears of reprisals such as under certain regimes. The problem is that in some cases anonymity is used by those who wish to commit acts that are either illegal or immoral without fear of being caught.

Activists involved in the Arab Spring often said that anonymity was essential to them. However, they did not actually want anonymity, what they sought was secrecy of their communications from the authorities. So what they needed was lack of association between their biological identity and the thing they were using for communication. Many of us achieve this by using different identities in different circumstances. We may use one name and email address for banking, another for gaming. We may have a home computer and a work computer. We use multiple identities in both the physical and online worlds.

One or many identities?

As already stated above, the subject of multiple identities is an area of rare unanimity of views, almost everyone is in favour of multiple online identities.

However, there are many people, particularly officials from repressive regimes who think that IPv6 (the new version of numbering that is being rolled out) will allow every individual to have their own unique identifier to use online and this would solve all the ID problems. But the reality is people do not want to be pushed to have one identity. They want a Paypal identity, a Google identity, a government identity, a Facebook identity and so on.

There is a very strong thread both in European and UN meetings on Internet Governance that says the misuse of information access and the ability to identify individuals, especially by oppressive governments, means 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. In the UK, there is a passionate concern by some people about anonymity. This tends to revolve around such things as online bullying of children and all aspect of defamation.

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.

This leads to the vexed questions of jurisdiction and how much personal information may need to be revealed to prove identity. These points are not covered here.

Conclusion

1. 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. There will never be global agreement on proportionality, but we should work towards global understanding of different perspectives and be able to accommodate most of them.

2. 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" of those services to come from targeted marketing and other sources.
3. Those who advocate the enforcement of strong, unique electronic identity for National Security purposes emphasise the advantages that anonymity in cyber space gives those with malicious intent:
   - Individuals can bully, stalk and libel; criminals can masquerade as valid customers, as acquaintances, as professional colleagues, or as real organisations in order to steal and defraud;
   - Terrorists can plan and co-ordinate atrocities, radicalise others, and undertake cyber-attacks on critical infrastructure;
   - Activists can damage the online presence of legitimate businesses, and publish confidential information;
   - Businesses and other States can engage in industrial, military and diplomatic espionage.

   All this can be done because anonymity removes accountability, and makes the job of law enforcement even harder online than it is in the physical world.

4. Those who oppose the imposition of electronic identity for national security purposes emphasise the advantages that **anonymity** in cyber space gives those with **good intent**:
   - Whistle blowers can expose wrong-doing by powerful individuals or organisations;
   - Individuals can partition their lives to limit intrusion by unethical organisations or damage caused by criminals stealing their identities;
   - Individuals can escape abusive relationships, hide from criminal or terrorist reprisals, avoid discrimination, or seek redemption by starting a new life;
   - Activists can organise and campaign against vested interests, giving voice to the otherwise silent majority; and
   - Governments, particularly democratic Governments, can be held to account, their policies challenged, and their mistakes or misdeeds held up for all to see.

   All this can be done because anonymity protects the weak individual from abuse by the powerful, and provides the transparency that holds the powerful in check.