Proving our identity online is a challenge we all face with increasing regularity. Having to go out of our way to prove our identity can be frustrating, so the prospect of being able to use our everyday web interactions as the basis for identification sounds appealing and convenient, but how robust and secure would this process be?

This article discusses how our online social footprint can be used as a means of identity verification and some of the pros and cons to this approach.
Peter Harrison, Product Leader in Identity and Fraud at Equifax, talked to Perspective about the ups and downs of using social media data when it comes to identity verification.

Proving our identity online is a challenge we all face with increasing regularity. Having to go out of our way to prove our identity can be frustrating, so the prospect of being able to use our everyday web interactions as the basis for identification sounds appealing and convenient, but how robust and secure would this process be?

This article discusses how our online social footprint can be used as a means of identity verification and some of the pros and cons to this approach.

Our online life is our identity

Interactions with friends, acquaintances, work colleagues, merchants, payment gateways, lenders and credit providers are increasingly happening online – and these interactions are often enabled or facilitated by social media sites such as Facebook, LinkedIn or Twitter, or by other entities that operate online, such as Paypal, Google or Amazon.

While these social media platforms have a purpose in their own right that we all use, enjoy and benefit from, a side effect is the wealth of information built up about us and who we are. Furthermore, because many of us have been using these social media platforms for a number of years, it means that there is now a depth as well as breadth of data that should be hard to fake.

Let’s look at social media data as a source of information for us to prove who we are and compare this to the more traditional means of verifying our identity.

Global coverage

The UK has mature and well-developed systems for recording and sharing information derived from our activities as citizens and consumers, such as the Electoral Roll, telephone directories, and records of the accounts we hold with banks, credit card providers, utilities, telecoms, media providers, insurers and so on. Typically this data is collated and held for sharing purposes by organisations such as credit reference agencies. In short, we live in a country where a significant proportion of the populace is credit active and has built up a relatively ‘thick file’ of usable information.

Yet even in the UK there is still a large number of people whose coverage in terms of these traditional data sources is thin, such as young adults, the ‘under banked’ and those who are ‘new to the country’. In other countries that do not record and share data in the same way, such coverage is even lower.

In contrast, the growth of the internet around the world with the increased prevalence, popularity and use of internet-enabled devices, such as laptops, tablets and smartphones, and of social media platforms means that there is large, and increasing, population coverage by social data. Furthermore, this coverage applies to most countries of the world, including those that are less economically developed and also amongst the more traditionally excluded communities.

The coverage of social data in the world is demonstrated in the graph (left), showing the leading countries based on the number of Facebook users.

Acceptance and popularity

The trappings of a consumer society have meant that many of us in countries like the US and UK have built up a strong profile of credit accounts etc, in order to enable us to acquire the things we need and desire – assuming we can afford them, of course. This data exists as a consequence of our participation in a credit-based economy and an acceptance of our role as a consumer within it.

A similar but more inclusive principle applies to social media. The use of platforms such as Facebook has grown exponentially over recent years because it feeds our basic human desire to communicate with other people; in other words, to socialise. It has the added benefits of being ‘always on’ (thus continually available), remote (suppressing inhibitions), and immediate (thus removing any natural ‘cool off’ period). These ingredients have fuelled its adoption. This data exists because of our preference, on the whole, to be social animals.

The strong and continuing worldwide growth of social media users is demonstrated in the graph overleaf.
Ease of use
The use of social media data as a means of identity verification has been developed by a number of organisations and has already been adopted by a number of service providers. The approach typically requires us to give our consent for the system to access and use our social media account data. Often to achieve a sufficient level of verification, this permission is required from multiple providers, as shown in the anonymised example below that uses a solution from Veridu.

While the prospect of needing to provide the details of multiple account logins appears onerous and overly disruptive, because we are actively accessing our social media accounts on our devices, it’s usually possible to sign in quickly and seamlessly via open authentication protocols.

Once the social media accounts are connected, additional authentication can be provided by challenging the prospective customer to prove their knowledge of their profile; for example, by identifying a named friend from a collection of profile photos.

Using this approach, our online identity can be scored in terms of its credibility. Furthermore, an assessment can be made of the ability for the identity to be faked. Clearly the greater the breadth and depth of the sources supporting the identity, the more difficult and time-consuming it would be to synthetically create it.

The ability of fraudsters to synthetically create identities that are seemingly supported by a broad range of social data sources cannot be disregarded though. Botnets can be ‘trained’ to create online profiles that look human, for example, by posting to social media sites at the times of day that we are most likely to be active, by using content from newspapers, books or other users’ timelines, by doing this over months, or by buying friends or followers and then sharing popular posts from the accounts to which they are connected. The sophistication of these techniques will only improve over time, allowing them to create seemingly realistic networks.

How ‘real’ these synthetically created profiles appear to be is open to question, however additional techniques like out-of-band authentication checks, such as the ‘spot a friend’ technique deployed by Veridu or the sending of a one-time passcode to a mobile phone or email address, will certainly help to counter this type of fraud.

Not got enough friends…
While a growing number of us are avid users of social media, it doesn’t mean that we all share the enthusiasm to live our lives so openly over the Internet. What happens if the identity verification process to enable you to use a particular service relies on your adoption and use of social media, and you are one of those people who, either deliberately or otherwise, abstain from the online world?

Recently reported in The Guardian was the case of a lady hoping to rent accommodation for a weekend away in Germany, but, on signing up to the peer-to-peer home renting website Airbnb and selecting a number of appropriate properties, she was continually rejected. When she followed this up with Airbnb, it turned out that she lacked a fully developed online identity. To quote the person involved:

“I’m a middle-aged mum of two, I’m a school governor, I have an impeccable credit record. But I couldn’t book a B&B. Not when I didn’t have enough ‘friends’.”

Eventually Airbnb was able to resolve the issue, but this highlights that, while social media adoption and use is widespread, it’s still by no means pervasive.

Idea in brief
THE SITUATION
Social media is a part of our everyday lives. What are the pros and cons – for businesses and individuals – of being able to use these everyday web interactions as the basis for identification?

THE CHALLENGE
While social media can be used to validate an identity, the rise of fraudsters creating synthetic identities means it’s not a fool-proof solution for organisations to rely on. And what about individuals who aren’t on social media or who don’t want to give organisations permission to access it to get data on them?

THE TAKE AWAY
Validating an identity to reduce fraud, protect consumers and improve the customer experience needs to look at several sources of information to ensure no-one is excluded from accessing products and services. But a solution that allows different touch points and layers for identity authentication is the most comprehensive approach.

Abstainers should not be excluded
For any identity verification process, the Holy Grail is the ability to be fully inclusive so that nobody is turned away because they don’t or can’t “participate” in society in the same way as most of us do, such as by choosing not to vote, to not take credit to fund their purchases, to not socialise via online media, and so on.

There have to be limits though. A person who decides to live their life completely “off the grid” cannot realistically expect an automated verification process to confirm the presence and ownership of their identity. Grizzly Adams need not apply!
Acceptance in regulatory markets
Identity verification is often required by organisations operating in regulated markets, where they need to carry out due diligence checks on prospective and existing customers to ensure they are not being used as a vehicle to fund illegal activities, such as money laundering. Would an identity verified solely on the basis of a range of online social media data be deemed sufficiently robust?

At the present time, probably not. If the process was augmented with more traditional data sources, like credit accounts, then this might be a more acceptable solution, in the short term at least.

Multiple layers for progressive authentication
The use of our online social footprint as a means of verifying our identity is a credible and robust approach that can stand alone in selected circumstances. Yet where a process needs to be inclusive of all members of society, such as those recently come of age, new immigrants, the under-banked, the elderly, the online abstainers, the socially excluded, and so on, we need to adopt a multi-layered approach that calls upon a variety of methods and data sources.

The method adopted needs to adapt to the circumstances. Questions need to be asked: What product or service is being acquired? What is the risk to the service provider? Do anti-money laundering regulations apply? Is the service being transacted online, over the telephone or via a face-to-face channel? How old is the customer? Are they registered to vote? Do they have a bank account? Is the customer transacting online with a trusted device? There could be many more questions to pose.

The identity verification process needs to adapt in-flight to address the circumstances as they arise. As part of this, the use of social media data becomes a layer to be used where most appropriate and when required; for example, if the prospective customer is relatively young and has a thin profile, for example with only lightweight credit accounts, that profile on its own might not be deemed sufficient evidence of their identity, given the risk associated to the product being acquired. However, when this profile is augmented with social data, there may be sufficient overall evidence to verify the identity.

Equifax Progressive Authentication enables risk-based adaptive identity verification and authentication based on multiple factors. The range of factors, or components, included in the platform will be extended over time, with a clear roadmap that includes the use of social media data.

For more information on our work in identity verification and fraud prevention, including details of our new Equifax Progressive Authentication solution, please contact Peter Harrison on 07887 596097 or email peter.harrison@equifax.com.