Introducing *Identity Plurality*

In security, we may be in the midst of a true paradigm shift, to a new worldview based on a plurality of identities. We've been saddled for years with the tacit assumption that deep down we each have one "true" identity, and that the best way to resolve rights and responsibilities is to render that identity as unique. This "singular identity" paradigm has had a profound and unhelpful influence on security and its sub-disciplines like authentication, PKI, biometrics and federated identity management.

Federated Identity is basically a sort of mash-up of the things that are known about us in different contexts. Its proponents often cite drivers licences and they way they're presented to boot-strap a new relationship. But it is a serious category error to abstract this case superficially to Federated ID, because while a licence might prove your identity when joining a video store, it does not persist in that relationship. Instead the licence is superseded by a new identity: that of a video store member.

A less trivial example is your identity as an employee. When you sign on, HR might sight your driver licence to make sure they get your legal name correct. But thereafter you carry a company ID badge – your identity in that context. You don't present your licence to get in the door at work.

Federated ID posits, often implicitly, that we only really need one identity. The "Identity 2.0" movement properly stresses the multiplicity of our relationships but usually seeks to hang them all off one ID. The beguiling yet utopian OSCON2005 presentation by Dick Hardt[1] shows vividly how many ways there are to be known, but he goes a step too far when he seeks to create a single, albeit fuzzy, *uber* identity that mops up all relationships and transcends all contexts.

An alternate view is that each of us actually exercises a portfolio of separate identities, switching between them in different contexts. This is not an academic distinction; it really makes a big difference where you draw the line on how much you need to know to set a unique identity.

Kim Cameron's *Laws of Identity*[2] promote the plurality of identity. They include a fresh definition of digital identity as "a set of claims made by one digital subject about itself or another digital subject". Cameron knows that this relativist definition might be unfamiliar; he recognises that it "does not jive with some widely held beliefs – for example that within a given context, identities have to be unique".

Ironically the singular identity paradigm may be a product of the computer age. Before the advent of "Identity Management", we lived happily in a world of plural identities. Each of us could be by turns a citizen, an employee, a chartered professional, a customer, a bank account holder, a credit cardholder, a patient, a club member, another club official, and so on. It was seemingly only after we started getting computer accounts that it occurred to people to think in terms of one primary identity threading a number of secondary roles. Identity management orthodoxy now insists on a singular authentication of who I am, followed by multiple authorisations of what I am entitled to do. The irony is that very modern advances like the Laws of Identity might take us back to the way identities were before the digital age.

Consider the importance of confidentiality in apomediation and online psychological counselling. Few will enrol in these important new patient-managed healthcare services if they have to identify themselves before providing an alias. Instead, participants in medical social networking will feel strongly that their avatars' identities in and of themselves are *real*.

The singular identity paradigm explains the surprisingly easy acceptance of biometrics. The idea of biometric authentication plays straight into the worldview that each user has one "true" identity. Biometrics' intuitive appeal must be based on an idea that what matters in all transactions is the biological person. But it's not. In most real world transactions, the role is all that matters. Only rarely—such as when investigating fraud—do we go to the forensic extreme of knowing the person.

There are grave risks if we insist on the individual being bodily involved in routine transactions. It would make everything intrinsically linked, violating inherently and irreversibly the most fundamental privacy principle: Don't collect personal information when it's not required.

Why are so many people willing to embrace biometrics in spite of their risks and imperfections? It may be because we've been inadvertently seduced by the idea of a single identity.

[1] http://www.sxip.com/videos

[2] http://www.identityblog.com/?p=354.