Volume **6** (1) 2024 https://doi.org/10.5204/lthj.3096

Why Are There So Many Digital Identities?

Mitchell Landrigan
University of Technology Sydney, Australia
Stephen Wilson
Lockstep Consulting Pty Limited, Australia
Hamish Fraser
Bird & Bird, Australia

Abstract

This article analyses why people have so many digital identities and offers suggestions to reduce the numbers to more reasonable levels. Paradigmatic digital identity thinking has been dominated by the objective of general purpose reusable identity as a response to the unwieldy profusion of identifiers that came with expanding ecommerce. The things called 'digital identity' in this paradigm are intended to be general purpose insofar as they are meant to be relied upon in different settings beyond the immediate control of the original issuer. The notion of reusable digital identity is somewhat intuitive, energised by the mental model of humans exercising a virtual self in cyberspace. Many user interfaces are constructed to exhibit an intentional stance suggestive of humans having a digital counterpart, making our digital actions more lifelike and comprehensible.

A reusable identity can limit inconvenience to end users and some of the risks of loss of personal data associated with end users creating multiple digital identities for discrete transactional situations. In some nations, there is a precedent for 'national identity', a concept that manifests as attributes necessary for a person to be identified or distinguished as a member of a state, typically to allow that person to be eligible to receive government services of the state. In these nations, national identity makes general purpose digital identity culturally more logical, even appealing. However, in most countries, the market for reusable digital identity is still not mature, except for low-stakes transactions, such as social media logins. To date, there is no solid business case for general purpose reusable identity—largely because it proves costlier than expected to re-engineer transactional identifiers to align (or federate) with an intuitive singular digital identity. Thus, individuals must manage many siloed, special purpose identifiers, account names, passwords and piecemeal authenticators.

If transactional identifiers go hand in hand with transaction systems, then there will likely remain a need for about as many identifiers as there are transactional services. Recent technology developments, especially in cryptographically verifiable credentials and mobile digital wallets, may provide ways to automate the management of multiple identifiers and achieve the desired usability anticipated from singular identity without disrupting the forces that have led to transaction-specific identification.

***Keywords**:* Digital identity; federated identity; personal identity; profiling.

Overview

The essay contributes to the existing field of research in relation to digital identity by providing an original explanation for why many people have so many digital identities. This article threads sociological, technical and economic materials with empirical information to propose that people have many digital identities because there is no solid business case or legal risk management model for a reusable digital identity. Economically important digital identities mostly relate to and derive from corresponding

business[1] applications and/or relationships. As a result of generally being unable to re-use a digital identity, people naturally need to have about as many different digital identities as business relationships.

The article uses the following structure to develop this thesis. The first section distinguishes *transactional* identity from personal identity and reviews the parties and processes in digital identity transactions. In the second section, the article explores the features of digital identity platforms, describing the dependencies between end users, service providers and identity providers in digital identity transactions. The third section reviews the evolution of digital identity, looking for themes that explain the unsuccessful commercial investments in digital identity platforms. The concluding section offers recommendations for accommodating a reality of multiple digital identities. Appendix 1 describes the technical features of digital identity systems in greater detail.

Transactional Digital Identity

Personal Identity and Digital Identity

Before investigating why people have so many different digital identities, it is necessary to distinguish digital identity from the sort of personal identity people are generally familiar with. Personal identity includes an individual's beliefs, perceptions, feelings, memories and aspirations that are shaped by their lived experience and fluid between social contexts.[2] A person may have different identities or personae depending on the social context the person is in. For example, in various social settings, the same CEO can be 'daughter', 'neighbour', 'former student', 'football club fan', 'Australian', 'Vietnamese–Australian' or 'aunty'. The individual may easily exercise different identities in these different social settings.

The fluidity of a person's identity in different interpersonal contexts is the result of personal identity being an individual *and* a social construct. There is a large body of literature describing the richness and fluidity of personal identity.[3] What might be described as 'social identity' also includes the identity of people in groups, typified by signs of 'belonging'. People in groups identify people in their own and others' groups by symbols of affiliation, such as connections with sporting teams (e.g., football club colours), countries (e.g., flags, flag colours), clubs (e.g., insignias), universities (e.g., logos, names, blazers), professional stars (e.g., T-shirts with pictures or names of pop stars, bands), etc.

Digital identity is a relatively new idea that has yet to achieve a widely agreed definition. Instead of debating definitions, this essay recognises two different senses of digital identity and focuses on the economically important one.

In one sense, digital identity is essentially a conversion of personal identity from the analogue or physical domain (often called the 'real world') to the digital domain (or 'virtual world'). As with personal identity, people can exercise multiple digital identities but with greater precision and separation. Indeed, one attraction of certain social networks is the facility for participants to adopt digital identities that are completely distinct from their real world identities, with benefits including a 'zone of privacy' to hold opinions and freely express views.[4] The concept of 'metaverses' makes this sense of digital identity all the more vivid; some researchers foresee the possibility of a profound future shift to literally living in a virtual world.[5] So, in this sense, people have different digital identities in much the same way as they have different real-world identities.

The other sense of digital identity is *transactional*. A transactional digital identity comprises the information that an end user must furnish about themselves to fulfil the requirements of a particular business application (using the term 'business' broadly to include social security services, health care, education and so on). A transactional identity often consists of simply a numerical identifier selected by the application provider to identify one customer within the set of all customers. The identifier in a digital identity transaction is a piece of information—it is a 'proxy'[6] for a person—and is not a person.[7] More technically,

[1]The terms "business" and "business application" are used somewhat broadly in this article to refer to formal activities (bound by rules) that a person conducts with businesses as well as governments, educational facilities, healthcare providers, and so on, by any electronic means, be that personal computer software, internet sites, or mobile phone.
[2]Identity cannot be separated from social power mechanisms: Al Tamimi, "Human Rights," 287.
[3]For contrasting views on personal identity, see Al Tamimi, "Identity as Theatre?"; Burke, Identity Theory, 129; Goffman, Presentation of Self; Jenkins, Social Identity, 39; Kwak, "If You Ain't First," 159; Mead, Mind, Self & Society, 176; Mir, "Digital Identity Evaluation Framework," 1; and Onitiu, "Incorporating 'Fashion Identity'," 108.
[4]Kaye, Report of the Special Rapporteur, 7; Dent, "Identity, Technology and their Confluence," 89.
[5]Chalmers, Reality+ (see, for example, 275, regarding the question 'is Data conscious?').
[6]Wilson, "Identities Evolve," 6.
[7]Noted, but not explored in this essay, is the question of whether a digital identity could have a separate legal personality, like a corporation: see Chesterman, We, the Robots?, 117.

digital identity is a 'sign, symbol or evidence … serving as proof of authenticity of identity', a 'token'[8] for a person's identity or for a transaction.[9] The digital identifier could be a biometric passport (or a biometric boarding pass[10]), an electronic licence, a passcode, a number, a face-recognising phone or a PIN for a debit card.

The transactional sense of digital identity aligns with the sort of digital identity framed by Kim Cameron in his seminal work 'The Laws of Identity' (*Laws*) as 'a set of claims made by one digital subject about itself or another digital subject'.[11] A transactional identity is not *meant* to be a complete description of the subject or customer but only suffices to enable a certain and sometimes narrow business application, such as banking, health insurance, health records management, student administration or licensing. Yet, granting people transactional digital identities can achieve measurable social benefits. The cited welfare benefits of giving people digital identities in poorer countries in the world include reducing election-related violence (Kenya, Mozambique), uncovering fraud in vote counting (Afghanistan), purging electoral rolls of people with invalid identities (Pakistan) and eliminating duplicate identities in electoral rolls (Nigeria).[12] These results have been made possible through digital technologies connecting targeted vital services for the first time to the hitherto 'unidentified'.[13]

Digital identity is not the same as a person's physical or biological identity although, as noted, digital identity systems may rely on biometric attributes of the person for authentication purposes, such as facial recognition or fingerprints. For example, the most extensive biometric-based identification program in the world, Aadhaar (in the world's largest democracy, India), relies on a combination of demographic and biometric information from end users for identification purposes. Aadhaar biometric identification comprises 10 fingerprints, two iris scans and a facial photograph for each person.[14] Aadhaar generates a 12-digit unique identifier, which the Unique Identification Authority of India issues to residents of India.

Before concluding this section on personal identity and digital identity, it is useful to describe two further concepts relevant to digital identity. First, 'general purpose reusable identity' is where identifiers and prior identification are reusable in different transactional contexts beyond the immediate control of the original issuer. Second, a 'national identity' comprises the attributes required for a person to be regarded as a member of a state, typically to qualify for eligibility for receipt of services from the state. National identity does not necessarily mean citizenship despite its intuitive connection to a person belonging to, or being a member, of a state,[15] nor does national identity imply nationalism. Instead, national identity is a prosaically impersonal concept: it is a token (e.g., a number) associated with the attributes required by a state for eligibility for services. Yet, having the attributes required for a national identity in the sense described here may contribute to the constellation of personal values associated with an end user's *personal* identity.

The relationship between general purpose reusable identity and national identity is an important one in a transactional sense. A national identity that is generally reusable can have beneficial implications for how end users manage their virtual identities. A national identity that facilitates end users' access to services in a reusable way can reduce the need for end users to create multiple digital identities for different transactions (assuming there exists a set of rules that support counterparties in those transactions relying on the national identity). A reusable identity can limit inconvenience to end users and some of the risks of loss of personal data associated with end users creating multiple digital identities for discrete transactional situations. Ideally, a national identity token is secure, resilient against counterfeiting and is not vulnerable to fraud, duplication or misuse. However, there are few instances to date of successfully federated national identities.[16] One striking example is BankID in Sweden, where end users can use their bank-issued identity token to digitally sign certain e-government forms and gain access to medical records. To be eligible for BankID transactions, the person must have a Swedish national identification number.

[8]Sullivan, "Digital Identity," 234.
[9]Sullivan, Digital Identity, 45.
[10]Brandler, "Air New Zealand."
[11]Cameron, "The Laws of Identity."
[12]The World Bank, World Development Report, 275.
[13]The World Bank estimated that in 2022, approximately 800 million people worldwide lacked identities; World Bank, Identification for Development, 11. One commentator has noted that in 2021, 3.4 billion people had a legal identity but had no way of using their identity online; Cooper, "Eligibility and Trust."
[14]Unique Identification Authority of India, "About Aadhaar."
[15]However, the Administrative Appeals Tribunal (Australia) has observed that, in relation to the Aadhaar identity regime, Aadhaar is intended to serve as proof of identity rather than citizenship or nationality; *1709985 (Refugee)* [2022] AATA 5089 para. 5.29. This case related to a protection visa sought by a person claiming to be a Nepalese citizen. Referring to the free movement of people between Nepal and India, the Tribunal observed that any person residing in India can obtain an Aadhaar card after 182 days of residence and that, while illegal entrants are ineligible to obtain an Aadhaar card, in practice, there is no verification against entry records; *1709985 (Refugee)* [2022] AATA 5089 para. 5.30.
[16]This is because even when given the option of reusing a national identity in business transactions, counterparties may not be fully confident in relying on identification performed by someone else, albeit the government.

Digital Identity Transactions: Parties and Processes

Most transactional digital identity is used to unambiguously index individuals in respective record-keeping systems and data-based services (i.e., customer reference numbers, government-issued identifiers, account numbers, licence numbers, passport serial numbers and the like). Usually known simply as identifiers, these have long been an inherent feature of any citizen or customer database. The use of identifiers predates the 'digital age' of the internet and contemporary digital identity frameworks. For example, charge card numbers were introduced in 1950 by Diners Club,[17] and social security numbers were introduced by the United States (US) Social Security Administration in 1936.[18]

The main parties involved in a digital identity transaction (i.e., the person being identified and the entity they are identifying themselves to) are, respectively, the 'subject' or holder of a digital identity (sometimes called the 'end user') and the 'relying party', typically a service provider that uses the digital identity to distinguish the end user of interest from all other possible end users. There are often intermediaries in this relationship—the 'identity provider', sometimes called the 'issuer'—that perform identification on behalf of others.

Trust Frameworks

There is a relationship between end users, service providers and identity providers that is often formalised in digital identity systems as a 'trust framework'. Service providers trust end users in a digital identity transaction insofar as the relying parties trust the identification done by identity providers (or else the service providers would perform the identification themselves). End users should be able to trust that service providers and identity providers will keep the end users' personal information secure and safe and that the information will only be used for the defined and understood purposes of a particular digital transaction. This point alludes to a tension, with legal implications, between the trust end users place in service providers and identity providers to use the end users' identity information for clearly specified transactions and the service providers' and identity providers' incentives to use the data for commercial purposes not authorised by the end users, including profiling and surveillance.[19]

Some trust frameworks are somewhat informal or implicit. For example, liquor stores and licensed premises almost universally rely on driver licences presented by customers as a proof-of-age token without any explicit contract. More important are the formal trust frameworks that set out explicit rules for using digital identities and credentials in a well-defined context. Such rules usually cover the identification protocols for registering end users, the terms and conditions for the use of digital identities and the liability protections afforded to relying parties when accepting such identities. Examples include the subscriber identity modules (SIMs) in a mobile phone network, website certificates used in the HTTPS (hypertext transfer protocol secure) web security protocol and the BankIDs Swedish banks issue to their customers that are used for e-government transactions.[20]

Federated Identity

A digital identity can sometimes be 'federated' across different identity management systems. In a federated identity management system, an identity provider performs identification of the end user and provides a reusable identity mechanism of some sort. In the highly popular 'social login' systems, Facebook (Meta), LinkedIn, Twitter (X) and the like act as identity providers, providing a token with which the user can log in to multiple sites using open access federation protocols, such as OpenID Connect (OIDC).[21] As noted, in more complex federations, like BankID in Sweden, end users can use their bank-issued identity token to sign certain e-government forms digitally.

---

[17]Diners Club International, "Join the Journey."
[18]Puckett, "Story of the Social Security Number."
[19]General Data Protection Regulation Article 4(4) describes profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." Gray, in "Taming the Electronic Genie," 4, describes surveillance as "the organised observation of behaviour with the aim of caring for, or controlling, the observed person." Bennett Moses, in "Data Problems and Legal Solutions," 10, notes "the potential abuses of a national scheme of digital identity based on facial recognition, the use of Facebook's powers of influence people to manipulate elections, and racialised impacts of predictive policing are all frightening because they involve potentially arbitrary exercises of power." In relation to concerns expressed by the Supreme Court of India about profiling and surveillance (including with respect to digital identities under the Aadhaar regime, where there are more than one billion registered digital identities), see *Justice K.S. Puttaswamy (Retd.) v Union Of India*, Supreme Court of India, Civil Original Jurisdiction, Writ Petition (Civil) No 494 of 2012 (Aug. 24, 2017), 241; and *Justice K.S. Puttaswamy (Retd.) v Union Of India*, Writ Petition (Civil) No 494 of 2012 (Sept. 26, 2018), 474. See also United Nations General Assembly, "Right to Privacy in the Digital Age."
[20]BankID, "The Digital ID Card Is Here!"
[21]OpenID, "Connect with Us."

In federated arrangements, the entities using the information relating to the attributes of a subject trust that those attributes are necessary to establish that person's eligibility for a transaction.[22] The parties agree (if not explicitly, then tacitly) that the subject can use the same identification token for different transactions. Federated identity management systems may enhance end user convenience (by reducing the number of separate digital identities the end user requires),[23] but liability in the event of misidentification can be complicated and, as a result, the extent to which a federated identity may be re-used can be restricted. With social login, the actions undertaken on the basis of a digital identity—namely logging into blogs, media and retail sites—are of little economic consequence, and social identity providers, such as Facebook, offer no warranty to relying parties. As a result, more-critical digital services, such as e-health and e-banking, do not accept social login. More sophisticated federations, such as BankID, are enabled by explicit legislation (e.g., Sweden's Payment Services Act (2010:751)) that confers certain powers on digital identities but, in turn, also tightly constrain the applicable usage.

The most ambitious identity federations, such as that of the US National Strategy for Trusted Identities in Cyberspace (NSTIC), envisaged unencumbered re-use of a digital identity across diverse domains, such as education, health care, banking and government. This has yet to prove feasible, as discussed later in this article.

Digital Identity Processes

Digital identity management systems also comprise underlying administrative processes. First, there is the 'identification'. This step involves identifying individuals as being (usually) unique within a given population or community. Once uniqueness is satisfactorily established, some sort of 'attributes' are usually assigned to them that are relevant for a given purpose (e.g., name, account number and registration number).[24] Next, there is 'authentication', which verifies that someone who is claiming to be a certain person *is* that person. Finally, for a person's identity to be digital, their relationship with others must be digitised. To digitise a relationship involves codifying certain things (attributes) that need to be known about the transacting parties and rendering those attributes in machine-readable form. Metadata is paired with the attribute information to help make the attributes dependable (e.g., the attribute source or issuer, the age of the attribute, and cryptographic signatures that bind data elements together).

Identification involves certain identifying information being checked by the issuer. The attributes assigned to the identified subject for use in transactions will typically be different to the identifying data. For example, the Know Your Customer (KYC) identification processes involve checking a candidate's official documents, such as passport and birth certificate, to establish a bank account. The attributes that are then assigned to the identified person and used as their digital identity need not (and generally should not) include the passport or birth certificate numbers. This is what is meant by the digital identity being a token of the person's 'real' identity—in other words, a *sign* that identification has taken place. In the case of banking, the attribute of bank account number is a sign that a KYC process has been undertaken, after which the customer can be referred to in the banking context by their account number. Authentication in banking (such as when processing a withdrawal) involves requesting the account number from a customer and applying some checks to verify that the account number belongs to the person presenting it.

In most cases, when a digital identity system is designed, the attributes requested or required in any given context are specified by the relying party (or on their behalf by an association or standards body) in accordance with the needs and risks inherent to that arrangement. The identification process that assigns attributes to end users is also specified when the system is designed. The nature and complexity of the information about the subject to support identification will vary from one type of transaction to the next. For instance, the information required from a new banking customer to open a savings account is typically more complex than the identity information required from someone who wishes to join an online social network.

[22]The concept of trust is inherent in digital identity transactions. There is (and must be) trust that: the correct entity holds the identity credentials being presented in each transaction; the communication will be unaltered and private; and the access control policy is not arbitrary and is implemented consistently throughout the enterprise; Windley, Digital Identity, 15. See also Organisation for Economic Co-operation and Development (OECD), Digital Identity Management, 10.

[23]Appendix 1 titled "Technical Features of Digital Identity Systems" considers this question in greater detail. Appendix 1 includes technical descriptions of three different identity management systems. The reader may wish to refer to those diagrams and return to this section.

[24]A drawback with conventional identity credentials is they can reveal too much information when used for a particular authentication purpose. For example, to prove that someone is over the legal drinking age, a bartender may ask to see a person's driver licence but the requirement to produce a licence needlessly exposes the full date of birth of the individual and other details, such as their home address, and can, thus, create security vulnerabilities. Digital credentials bring the useful possibility of more selective disclosure.

Economic Requirements

As context for why there is no business case for general purpose reusable identity, it is useful to describe the economics of digital identity platforms. The commercial viability of investment in an identity management system depends on the identity provider, the service provider and the subject (end user) benefiting from transactions over the system. Investment in digital identity infrastructure is a finely balanced equation. There must be a net marginal benefit among the three parties from having the service rely on the identity provider's identification of the end user accessing the service.[25] End users must, on the whole, gain from ease of use, service quality, access to more services, or improved security of their data.[26] The service provider must realise the benefits of using the system, for example, by being able to reach larger markets.[27] The identity provider must gain through receiving a reasonable fee for the service.[28]

The Organisation for Economic Co-operation and Development described the economic dependency between service providers and end users in relation to digital platforms as a 'circular situation', whereby:

> On the one hand, service providers are holding back from investing in new services until a critical mass of individuals use strong authentication credentials and, on the other hand, individuals are waiting for a critical mass of services that require strong authentication before they adopt the technology.[29]

The role of identity provider is not specifically mentioned in the above passage but should be thought of in this context as the unnamed provider of 'strong authentication credentials' and 'technology'. The 'circular situation' means that economic returns for commercial identity providers remain uncertain while service providers and individuals alike are still waiting. This argument is confirmed by practical experience in the United Kingdom (UK) and the US, where no commercially sustainable identity providers have yet to emerge in the wake of public–private investment (as discussed in the later section titled *Unsuccessful Digital Identity Investments*).

Demand from end users for commercial identity services will depend on the risks and benefits (including ease of use) that end users perceive or experience in acquiring digital identities. An end user may have little choice but to supply prescribed identity information to acquire a government-issued identity, but governments tend to hold all necessary identification data already. The value of an identity service for an end user will hinge at least in some part on the confidence that the end user has about the security of the identification information to be supplied to the identity provider and the cost of furnishing this information relative to the quality, price and scarcity of the service.[30] Therefore, end users implicitly weigh up the value of the service and the cost of what they are potentially risking when disclosing their identity information to acquire a service.

Demand from service providers for commercial identity services hinges on realising a net cost saving from, in effect, outsourcing identification to a third party. For low-risk service providers, such as media and blog sites, the decision to outsource identification to social login providers appears to be simple, insofar as logging in with a Facebook, LinkedIn or Twitter account are enormously popular choices. In these cases, the identity providers make no claim about who a user really is and provide no warranty for the correctness of the identification. In fact, the 'identification' is rather trivial; the main operational benefit of social login is a reasonable assurance that whoever it is that logged in on any occasion is likely to be the same person on each occasion. That is, a service provider is comfortable relying on social login when they (the service provider) do not much care who the user really is. Relatively little is at stake in these transactions. Demand from service providers for free market identity providers in higher risk–transaction settings, such as e-health and e-government, has proven too small for commercial sustainability.[31] Only under artificial identity market conditions—such as Sweden, where legislation enables BankID to be used for particular (not all) government transactions—does federated identity provision become a commercial proposition.

[25]Landau, "Economic Tussles," section 6.
[26]Landau, "Economic Tussles," section 6.
[27]Landau, "Economic Tussles," section 6.
[28]For the purposes of this economic analysis, the "free" social identity providers, such as Facebook, LinkedIn and Twitter, are ignored. Social networks offer these services for indirect gains, such as the acquisition of additional customer information and insights, including usage data.
[29]OECD, Digital Identity Management, 12.
[30]It is assumed here that the end user has a choice about whether to use the service.
[31]See the NSTIC and Verify discussions below.

Evolution of Digital Identity

Having surveyed some of the social, technical and economic aspects of digital identity transactions, this section of the article maps the evolution of digital identity. This part also describes examples of unsuccessful commercial investments in digital identity approaches and technologies, often resulting from overly general or expansive attempts to deal with people on the basis of a general purpose identity.[32]

The evolution of digital identity theory and practice provides important insights into the dynamic relationship between service delivery (which is increasingly digital) and risk management in delivering services to the right recipients. Historically, matching services to recipients in the analogue world was done with the benefit of social cues and identification customs; when in doubt, experienced service personnel have a range of ways for detecting attempted fraud and double-checking who a customer is. Yet, these mechanisms break down in the digital realm.

Over time, it became apparent that the success of a digital identity initiative depends on including the perspective of relying parties because they tend to bear most of the risk of misidentification (insofar as the consequences of identification errors tend to have the greatest effect on relying parties). Initial attempts to digitise customer service were based on an intuitive drive to convert the personal identity to a holistic digital equivalent. But as digital services become more complex, it follows that the things that a service provider needs to know about a recipient become more and more specific. For example, entitlements to health care online today can depend on vaccination status, location, citizenship, the timing of Medicare rebate conditions and so on. Consequently, digital identity mechanisms have evolved from general identity to sets of fine-grained attributes. Credentialing technologies have evolved at the same time towards selective disclosure of verifiable details of a person.

To provide further context to how digital identity evolved to what it is today, it is also useful to note the difference between a *thing* and the *name of that thing* and, similarly, to observe the distinction between a person and how that person is known or referred to. These two different perspectives of 'identity' become somewhat clearer in the digital domain, if only because in the digital world, the only thing available is information. With the advent of the internet and widespread day-to-day electronic activity—in other words, cyberspace—a great deal of people's regular identity has been made digital, and several new dimensions have been added. However, these are still the early days of digitisation. Only relatively recently is there a generation of adults who have not known 'snail mail', fixed-line telephones or free-to-air television; yet almost all economically important digital activity is still rooted in an earlier generation of norms and regulations.

Online state-sanctioned processes often ask for identification details, such as a driver's licence, social security number and passport. Yet, this information is at risk of theft and criminal use; it is better for an end user to be asked to prove their identification details but for the details to be scrapped once checked (or suppressed altogether). The state of the art in digital identity proofing—including Australia's Document Verification Service and the US electronic Consent Based Social Security Number Verification service—involves application programming interfaces through which eligible organisations may request verification of given government documents against official registries. These systems have brought conventional KYC processes from the analogue to the digital domains, with no essential change to the meaning of the base documents, and at the same time, reduced the handling and copying of sensitive customer documents.

The 'Standard Model' of Digital Identity

Since 2005, the digital identity industry and most government 'trust frameworks' have been based on what can be called the 'standard model', handed down in *Laws*.[33] Cameron had emerged from Microsoft's unsuccessful Passport initiative of the early 2000s with a fresh determination to forge a digital identity program that was non-proprietary and sufficiently abstracted to be able to suit a wide range of businesses and transaction types in need of identification and authentication. Cameron convened numerous informal collaborations and first revealed the *Laws* in a series of blogs. As noted, *Laws* defined digital identity as 'a set of claims made by one digital subject about itself or another digital subject' and formalised a number of participants in what Cameron called the 'identity metasystem'. These parties were primarily, returning to the nomenclature introduced earlier: the subject (end user; the party who is identified), one or more identity providers (entities that perform identification on behalf of others) and relying parties (usually service providers; entities that rely on the identification of a subject to transact with that subject).

[32]The next section gives the pre-eminent example of a successful broad-based digital identity standards initiative.
[33]Cameron, "The Laws of Identity."

While in the abstract, it is reasonable to see banks, government agencies, professional associations and so on as 'identity providers'—insofar as they vouch for sets of claims about individuals, and those sets of claims are, under the *Laws'* definition, 'digital identities'—the Standard Model created the express expectation that these sorts of institutions could and should become overt *providers* of a new type of good called 'digital identity'.

In the wake of the *Laws*, many institutions and associations tried and failed to forge new businesses providing digital identity. Examples included the Australian banking sector The Trust Centre,[34] various post offices and many start-up businesses. Few of these ventures have survived as commercially sustainable identity providers. Several well-funded public–private partnerships came and went, including the NSTIC and GOV.UK Verify,[35] both reviewed in the next section of this essay. The governments of Australia and Canada continue to work on 'trust frameworks' based on the Standard Model: the Trusted Digital Identity Framework (TDIF) and the Pan-Canadian Trust Framework, respectively. Despite substantial seed funding, few, if any, commercially sustainable identity providers have emerged.

Limitations of Reusing Digital Identities

There is also a strong in-principle drive (on both the supply and demand sides) to re-use established identification when creating new accounts. Federated identities established in one domain are expected to be recognisable and reusable across other domains. Conversely, fresh identification is expected when creating new accounts in some sectors—most notably banking, with its strict KYC rules. If one service provider has established a customer identity for its own purposes, then it will not usually be comfortable having that identification relied upon entirely by other services because the consequences of, and liability for, misidentification are difficult to contain or even to define.

As a result, end users must re-establish the bona fides with each new service, resulting in different passwords and online login protocols for travel, banks, social media, credit cards and for paying utility bills. Online, individuals experience the inconvenience of multiple accounts. The need for a different password for each account is potentially difficult for some people to manage; yet reusing passwords across accounts is a security risk. Finding solutions to the problems of managing multiple passwords can create new complications. For example, password managers are not immune from security breaches[36] and can become a single point of security failure. Personal information collected for discrete identification purposes is vulnerable to security breaches and accidental loss, potentially leading to subsequent identity-related fraud through the criminal re-use of such data to establish fake identities or to gain access to existing accounts.[37] The ability to re-use personal information without the consent of end users makes that information valuable to criminals and potentially propels a black market in stolen data.

The primary means for protecting access to online accounts is the password, a creation of 1950s-era computer systems administration, designed by engineers for engineers. Passwords are supposed to be difficult to use. This creates a unique paradox: no other consumer technology has an effectiveness that is inversely proportional to its usability (i.e., the simpler and more usable a password is, the less safe or effective it is). In cybersecurity, single-factor password authentication (which hinges on a singular secret or 'something I know') is sometimes augmented by additional factors, such as a physical token ('something I have') and/or a biometric ('something I am'). For many years, such multifactor authentication (MFA) required (and still requires) special purpose peripherals like smartcards and readers or one-time password generators, which are awkward to use and, in the case of one-time password generators, provide questionable net benefit.

The state of the art in contemporary MFA uses mobile phones where the phone itself is the second factor, known to have been unlocked by a match-on-device biometric or PIN. The FIDO Alliance[38] is an authentication industry standards body established in 2013. It is responsible for a series of protocols that have been ratified and published on an unencumbered (open) basis by the World Wide Web Consortium (W3C). FIDO is arguably the most significant identity industry initiative of all time, in part due to significant membership representation by relying parties (including large financial institutions, such as Bank of America, Mastercard, PayPal and Visa; insurers, such as Aetna; and retailers, such as Alibaba and Amazon). FIDO has seen MFA and 'phone as second factor' adopted by numerous major services and products, including Windows Hello and Samsung Pay. Mobile phones with sophisticated FIDO-capable, built-in cryptographic processing are increasingly common and are almost always close at hand. Therefore, it is reasonable to install mobile device MFA into routine authentication so that people can

[34]Finextra, "Westpac Backs Customer ID Management Initiative."
[35]For further details, see the section titled "Where Have Digital Identity Investments Been Unsuccessful?"
[36]Touba, "Security Incident Update."
[37]See Australian Government, Department of Prime Minister and Cabinet, Connecting with Confidence, 10. Ryan, in Trust and Distrust in Digital Economies, 228, observes that: "[i]n a time where identity theft of both the living and the deceased is rife, the rights of deceased whose personal data security has been breached will be fertile ground for future litigation."
[38]FIDO Alliance, "Simpler, Stronger Authentication." FIDO stands for fast identity online.

'identify' across multiple platforms, leveraging the facial recognition or other authentication features used to unlock their phones, together with additional layered authentication signals (e.g., geolocation), which can help improve confidence that the digital identity, kept safe in its data carrier, is in the right hands when presented.

Identity Federation Paradigm

Today, digital identity businesses and government policy alike are generally shaped by the paradigm of identity federation. Running through almost all initiatives is the assumption that digital identity can be re-used across transaction domains or business contexts. It is assumed there will be a significant pool (i.e., a marketplace) of service providers (relying parties) for which formally codified digital identities will be meaningful, *and* there will be a range of identity providers, each willing to vouch for identities used by those service providers.

The things called 'digital identity' in this paradigm are intended to be general purpose insofar as they are meant to be relied upon in multiple contexts beyond the immediate control of the original issuer. This concept of identity federation is exemplified in practice by 'social login', the widespread method of using a social media account or 'handle' to gain access to another website or to enrol in a new service. Social login almost always uses technical federation protocols, such as OIDC or OAuth 2.0 (Open Authorisation), in which web servers exchange messages that prompt the user for permission to share certain pieces of data and relay that data from the social media 'authentication service' to the destination web server. This experience is now commonplace on the internet and has come to represent one of the most practical benefits of Facebook, Google, Twitter and the like. Further, the social login experience is so well habituated that it has informed federation proposals at the highest levels. For instance, when the Obama White House launched NSTIC in January 2011, the President's Cybersecurity Adviser, Howard Schmidt, envisaged that the strategy would spawn an 'ecosystem' in which:

> [a] student could get a digital credential from her cell phone provider and another one from her university and use either of them to log-in to her bank, her e-mail, her social networking site, and so on, all without having to remember dozens of passwords.[39]

Yet, this federation across education, banking, healthcare and government sectors has generally failed to move significantly beyond the easy cases of social login to low-stakes websites. If it turned out that the student in Schmidt's vision was misidentified by her cell phone provider or university, and the student went on to cause losses or other damages at her bank, it has never been entirely clear what sort of legal action is available to the bank against the original identity provider. With uncertainty hanging over liability in identity federation, it has been difficult for banks, universities or telcos, and even governments, to build 'identity businesses', irrespective of how much demand there may be from consumers for a better authentication experience.

One observation about digital identity platforms is that digital identity is potentially not the sort of thing that is merchantable, at least not in its own right. This is not to say that digital identity is not valuable; rather, its value may need to be realised in indirect ways. The digital identity industry and field of practice are already adapting to this reality, with the evolution of services towards cryptographically verifiable credentials.[40] These are generally digitised versions of existing real-world credentials, rendered in a tamper-resistant format bearing the digital signature of the credential issuer to evince provenance. Verifiable credentials are usually presented together with the digital signature of the credential holder created securely within the holder's digital device to provide evidence that the credential was under the control of the right person.

The same cryptographic technology, now widespread in mobile phones, that enables FIDO authentication also enables verifiable credentials (i.e., public key cryptography and digital signing in tamper-resistant mobile secure elements). Verifiable credentials are being used to convey the holder's specific attributes, not the holder's personal identity. The World Health Organization exemplifies this trend with its published guidelines for digitised COVID-19 certificates, which expressly recommend against treating a digital vaccination certificate as an 'identity'.[41] The major mobile wallet platforms of Apple and Google—widely used for mobile payments using virtualised credit cards—are being extended to use the same cryptographically secure elements and contactless radiofrequency interfaces for handling other virtualised credentials, such as digital driver's licences.[42]

[39]Schmidt, "Enhancing Online Trust and Privacy."
[40]See World Wide Web Consortium, "Verifiable Credentials Data Model."
[41]World Health Organization, Digital Documentation of COVID-19 Certificates.
[42]Apple, "Driver's Licenses and State IDs in Apple Wallet."

Unsuccessful Digital Identity Investments

Around the turn of the 21st century, as the importance of the internet for commerce and administration became apparent, governments grappled with their role in regulating and enabling this new technology environment. Some countries saw benefits in public key infrastructure–based digital signatures and granted this technology special standing. Malaysia, for example, enacted the Digital Signature Act 1997 (effective 1 October 1998), the first such national legislation in the world. Similar statutes followed in Italy and elsewhere.

Other countries tended to take a deliberately light-touch approach towards digital identity, expecting that the free market would look after authentication and identity, just as it was cultivating great innovation in internet technologies. Thus, the British Cabinet resolved to '[look] to the establishment of a range of authentication services by central and local government and the private sector, and for public sector bodies to use these'.[43] Similarly, the US National Institute of Standards and Technology (NIST), when establishing the NSTIC in 2012, predicted that the 'vibrant marketplace created by the Identity Ecosystem will provide people with choices among multiple accredited identity providers, both private and public, and choices among multiple credentials'.[44] There are comparable technology-neutral, laissez faire approaches at work in the government regulatory strategies of Australia, Canada and New Zealand.

Yet, it appears that no commercially sustainable identity services have emerged through free market forces in Australia, Canada, New Zealand, the UK or the US. This is despite the near universal acknowledgement that digital identity is critical to the digital economy. For example, consider GOV.UK Verify, a planned private–public partnership to stimulate a digital identity marketplace, seeded initially by demand from dozens of British government agencies. Verify began prior to 2014 with a series of government-funded trials conducted in anticipation of a panel of government-approved identity providers emerging. A long series of missed milestones followed. By 2018, less than half of the expected 40 government services had adopted Verify, and by 2020, only 5.4 million end users had signed up, compared with a target of 25 million. An official investigation was conducted by the National Audit Office, and funding for Verify was eventually stopped in 2020. The total expenditure by the UK Government Digital Service (GDS) over 2016–2020 was reported to be GBP154 million, with a forecast economic benefit initially forecast to be GBP873 million.[45] In 2019, GDS revised its estimate of the benefit down to GBP217 million, a shortfall of GBP656 million. On the supply side, the true cost of Verify exceeds GBP154 million, because GDS reporting does not include costs to agencies of switching to the new system.

It had been expected that Verify might continue after government funding was stopped, on the strength of the purported demand for digital identity. Yet in 2022, the government announced that all Verify services would close in April 2023.[46] The cost of building Verify is comparable to the revised economic benefit figure, and the unquantified cost of inconvenience to end users and the forced move for agencies to revert to their own identity solutions makes the equation far worse. There was a major negative direct economic effect from the investment of GBP154 million.

Turning to the NSTIC, the total expenditure for the US NSTIC program can be estimated from the publicly known pilot grant outlays (namely, USD30 million[47]) plus the ongoing funding appropriated in the NIST budget for the NSTIC National Program Office. In a typical fiscal year (e.g., FY2012), the National Program Office cost approximately 40% of the grant outlay.[48] It follows that NSTIC cost approximately USD42 million. Few, if any, commercially sustainable identity providers resulted from NSTIC. While it is important to acknowledge that indirect benefits would likely have flowed to the 20 or more grant recipients and to industry more broadly, the promise of NSTIC was explicit: seamless interoperability of login credentials across education, mobile phone accounts, banking, email and social networking. Relative to the objective of cross-sector, national scale federated identity, the USD42 million cost of NSTIC was arguably entirely wasted.

Efforts continue with the Pan-Canadian Trust Framework and Australia's TDIF. Neither of these projects can be regarded as failures (yet), but they have taken many years longer than expected to produce any significant rewards. The cost of TDIF and the associated myGov single sign-on system had exceeded AUD200 million by 2019.[49] It is unclear whether these projects will generate any net benefit. The premise of TDIF, as with GOV.UK Verify and NSTIC, has been that the private sector would

[43]Central IT Unit, e-government, 19.
[44]NSTIC, Recommended Charter, 2.
[45]National Audit Office (UK), Investigation into Verify, 7.
[46]UK Government, "GOV.UK Verify is Closing."
[47]Megas et al, NSTIC Pilots, 1.
[48]National Institute of Standards and Technology, Overview of the Fiscal Year 2012 Budget.
[49]Hendry, Justin, "Australia's Digital Identity Bill."

deliver commercially sustainable digital identities, yet the Australian government has had to draft digital identity legislation[50] to facilitate interoperability with private businesses and state governments. The draft legislation has not progressed substantially since 2021.

A Suggested Way Forward

Does it matter if people have many transactional digital identities?

Perhaps not. The former Technical Architect for Identity Assurance at the UK GDS, Adam Cooper, suggested in 2021 that identity is only a means to an end when he said, 'most people don't care about digital identity; they just want better access to services'.[51] End customers may not require any more than good access to services, albeit with multiple different identities managed across many different digital platforms. Mobile technology can and should 'abstract away' the transactional digital identity from the user experience by automating the use of the appropriate identity in a digital wallet for the service of interest. Notwithstanding the theoretical aspects of identity, there is a clear need for a better authentication experience for end users in cyberspace. Securely logging in to secure websites and services is inconvenient and difficult;[52] people struggle with too many passwords, and recovering forgotten passwords often spoils the online experience. The cumbersomeness of managing multiple digital identities can also extend beyond death; any person with many digital identities in life also has many digital identities for others to disable or deregister after the person dies. Personal data can be stolen; it is relatively easy for criminals to impersonate and defraud individuals.[53] Payment fraud has moved to the internet card-not-present channel because chip technology has successfully curtailed card-present fraud.

One potentially preferable option to the current mix of multiple digital identity platforms would be to automate authentication (such that online services can tell that the right user is on the line without the user needing to enter a password or select a credential) and equip each end user with a digital wallet holding diverse verifiable credentials. Installation of credentials would follow the same secure protocols used for installing virtualised credit cards, boarding passes and COVID-19 certificates. Software could then invoke the correct verifiable credential automatically for whichever service the user is attempting to reach. Consider how useful information, such as a date of birth, is packaged within a driver's licence or passport today. Digital technologies can allow these facts to be presented selectively, without exposing irrelevant personal details, and ingested automatically by relying parties, with automatic verification that the details have not been tampered with and have indeed been presented with the consent of the rightful holder. End users appear to have clear mental models of their entitlements to certain services—they know what their credit cards, healthcare card, driver's licence and loyalty cards mean and which services or capabilities these credentials correspond to—and these mental models are not necessarily primarily about identity. Furthermore, large and growing sections of the populace are increasingly comfortable with digital mobile technologies; that is to say, sophisticated cryptographic technologies have been made into consumer products. Once digitised and securely stored under their owner's control, credentials should be recognisable by application software so that the appropriate access to digital services is opened up automatically.

Clearly, the adoption of digital technology is far from universal, and a digital divide puts many people at a significant disadvantage. Yet, this imbalance affects people on a broader level than just 'digital identity'. Access to any service—be it related to government, finance, health, media or transportation—is increasingly mediated digitally. Consequential inequality is a pressing social problem. The digital divide is only going to worsen if digital identity remains piecemeal, difficult to use and unevenly secure. If mobile digital wallets with built-in cryptographic technology can effectively automate the reality of multiple transactional identities to improve security and privacy, then these capabilities should be made more readily available.

[50]Australian Government Digital Transformation Agency, Digital Identity Legislation.
[51]Cooper, "Eligibility and Trust."
[52]Summarised as "cumbersome user experiences": Boston Consulting Group and walt.id, Me, Myself and (SS)I. Appendix 1 titled "Technical Features of Digital Identity Systems" considers this question in greater detail.
[53]OECD, Digital Identity Management, 7.

Appendix 1: Technical Features of Digital Identity Systems

This appendix describes the technical features of digital identity systems by referencing three digital identity management models.[54] It concludes with a summary.

Centralised Identity

As shown in Figure 1, centralised identity is where an organisation (relying party) creates an identity token directly with the subject (end user), which allows the subject access to the relying party's service. For example, the identity token could be a passcode, an authenticator app on a mobile phone or a physical electronic key. There may be additional confirmation information required from the subject, such as the subject being asked to return a random code sent by SMS to the subject.

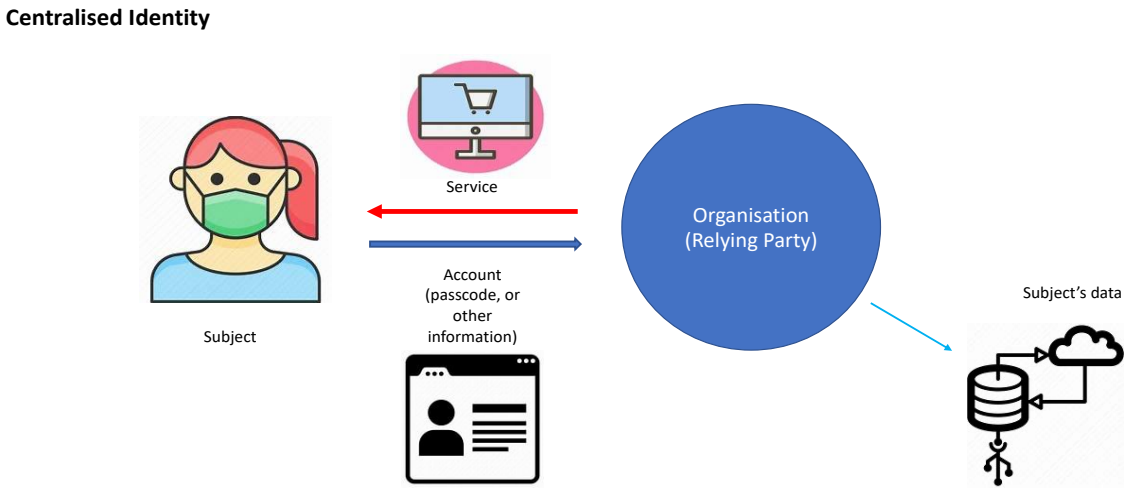

Figure 1. Centralised identity

In this example, the subject wishing to access a relying party's service will present an identity token specific to that relying party. This simple observation reveals a core limitation of the basic centralised model. A subject may have to maintain many—perhaps hundreds—of passcodes and authenticators, one for each different relying party. Recording, storing or memorising passcodes may be an inconvenience for the subject. Worse, if the subject uses the same or similar identity passcodes with multiple relying parties to avoid or limit the drawback of maintaining multiple passcodes, this may create security risks.[55] Namely, if the subject's passcode is hacked, then there is a potentially greater risk of unauthorised access to more than one of the subject's private accounts. Implicitly, the subject must make a choice. The subject can maintain fewer passcodes but face security problems if their repeatable identity tokens are hacked, lost or stolen. Alternatively, the subject can bear the relative inconvenience of managing multiple passcodes but, by doing so, may better manage the risks associated with multiple security breaches.

It is worth also noting that the identity token in a centralised identity management system in and of itself usually represents very little 'identity' information, or sometimes none at all. A typical token is a meaningless string of characters forming a secret passcode or an unmarked passcode-generating key fob. The identity token represents a kind of proof that the holder of the token (i.e., the subject) was at some time identified to the satisfaction of the relying party and provided with the token. Presentation

[54]Figures 1, 2 and 3 and the descriptions for each figure draw on the helpful articulation of digital identity frameworks prepared by Hamilton Duffy, "Decentralise What?".
[55]Organisation for Economic Co-operation and Development, Digital Identity Management, 11. See also Apple, "macOS User Guide," and Google, "Passwordless Login with Passkeys."

of the token subsequently is taken to mean that the proper subject is present and may be granted access. In any other context, the identity token should be meaningless; in particular, the token alone provides no identity information about the subject.

Federated Identity

Another kind of digital identity transaction is shown in Figure 2. Here, an identity provider is the interface between the subject and the relying party. The identity provider performs the initial identification of the subject, provides them with an identity token and 'federates' that token using open access protocols so that the subject can access one or more relying parties' services.[56] For example, the subject's social network identifier may allow the subject to access another social or media network. In contrast to the centralised model, a federated arrangement may improve the subject's online experience by helping to reduce (or, more accurately, not add to) the number of usernames and passcodes that the subject needs for identity transactions. A feature of the federated model is that the subject may not know until they enter a transaction that the transaction *is* a federated arrangement.

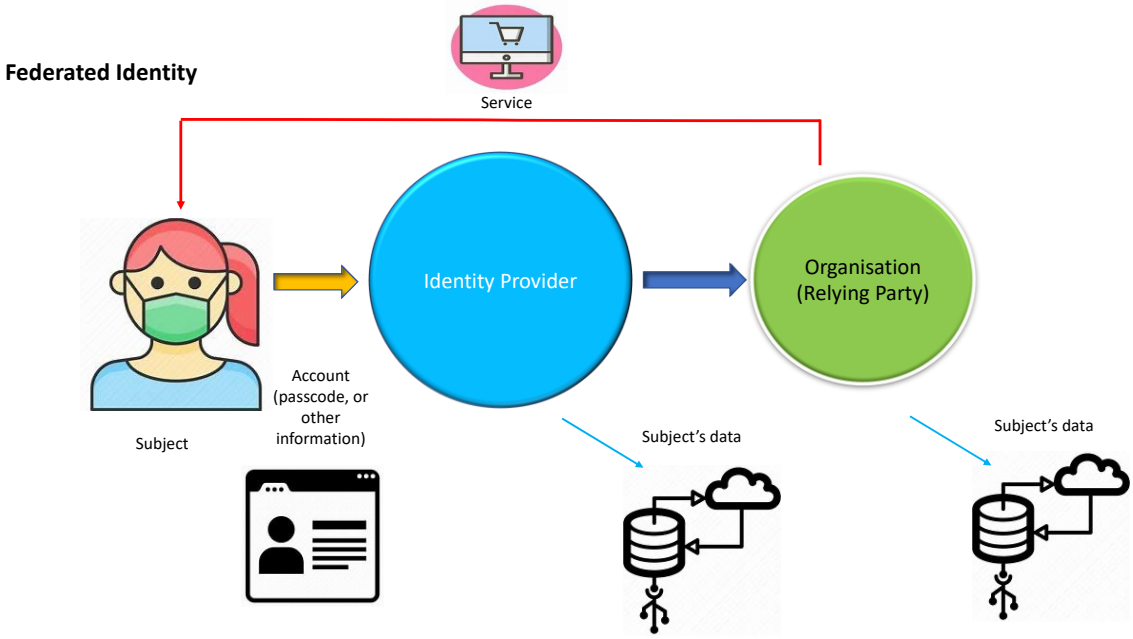

Figure 2. Federated identity

There are complex forms of the arrangement described in Figure 2 in identity systems that provide multiple services in a federated but centralised model. The digital identity platforms in multiservice centralised social welfare systems (e.g., public health services and social service benefits) are typically government-backed and require a subject to verify their identity to the government service provider by producing a recognised token or code that the subject has first obtained from a government authorised identity provider.[57] Once the subject obtains the token, the subject can use the token to identify themselves to seek to acquire the government services. A single token may facilitate end users' access to many government services.[58] It is not

[56] As is the case with the centralised model of identity, the identity provider may require the subject to strengthen their identity information with additional security information to satisfy the requirements of other organisations (i.e., other relying parties).

[57] For example, the Australian Government allows a person to create a digital identity using a "myGovID" to access services, such as Medicare, Centrelink and the Australian Tax Office, as well as 80 other services: see Nabben, "Government Wants to Expand the Digital Identity System." In the case of myGovID, a "standard" identity strength requires the applicant to supply two documents, such as a passport, birth certificate or driver's licence. By contrast, a 'strong' myGovID identity strength requires the applicant to furnish a passport (not more than three years expired) and a birth certificate, citizenship certificate, driver's licence or Medicare card, as well as submitting a face verification check. The type of myGovID determines the kinds of government services that the person has access to.

[58] For a history of Australia's political experience with identity regimes (including the Australia Card in the 1980s), see Jordan, Identity Cards and the Access Card. The World Bank observed in 2021 that "rather than more traditional models with a single central ID provider (IdP), a number of countries have developed federated ecosystems of multiple IdPs that provide government-recognized identity verification services governed by a trust framework"; The World Bank, 2021 Annual Report, 11. This [the World Bank observed] "offers potential benefits (such as increasing choice, competition and innovation), but also involves a number of challenges (such as the capacity to effectively develop and supervise regulations and standards)"; The World Bank, 2021 Annual Report, 11.

unusual for there to be rigorous identification requirements for end users to obtain a token. Government identity providers and service providers have a legitimate interest in ensuring that they are dealing with the right people before authorising them to have access to services funded by public money.

In a federated system, a government-issued digital identity may also serve as partial identification for the purpose of other digital identities or relationships. In Australia, for example, the Australian Business Registry Services administers director identity registrations.[59] The directors of most corporations, including (regardless of where they live) a director of a foreign company registered with the Australian Securities and Investment Commission and conducting business in Australia, must apply for and obtain a director identity.[60] The most straightforward way for a company director to apply for a director identity is to use their existing myGovID (a general purpose digital identity) and supplement it with director-related details. For example, a director with a 'strong' myGovID[61] need only support their identity application with a company tax file number or their residential address registered with Australian Securities and Investment Commission.[62]

Decentralised Identity

A third, more recent, system is *decentralised* identity management (see Figure 3). This model has the claimed benefits of allowing subjects to have better control over at least some of their data and of permitting service providers (the 'Verifier' in the below diagram) to only obtain the minimum amount of information from the subject that the service provider requires for a particular transaction. This model proposes that the subject interacts directly with verifiers. Those verifiers are the same service providers who are described in the earlier diagrams.

The subject can authenticate their identity directly with the relying party, or there can be mutual authentication. In keeping with the philosophy of decentralisation as a means to reduce reliance on government and institutions, a distributed ledger or blockchain usually anchors the metadata, such as public keys and credential identifiers necessary in transaction software for verifying identity and establishing trust; however, the decentralised identity standards tend to also allow for regular databases and government registries.[63]

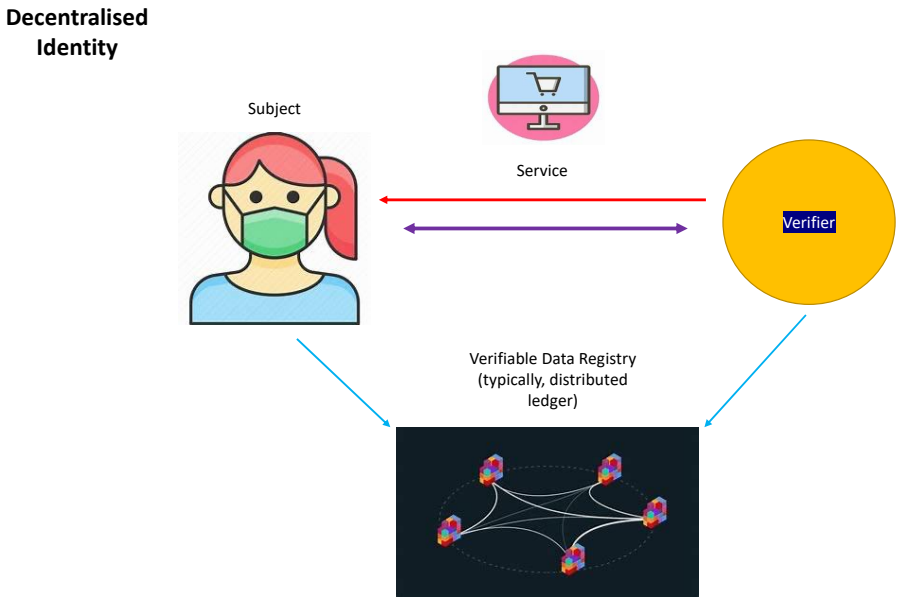

Figure 3. Decentralised identity

[59]There are fines for directors for failing to obtain identities; failing to apply for identities; failing to produce identities when required; and applying for multiple identities: see sections 1272C, 1272D, 1272G and 1272H of the *Corporations Act 2001* (Cth). The primary purpose of the identity regime is to prevent the use of false or fraudulent director identities.
[60]Australian Securities & Investment Commission, "Director Identification Number."
[61]The myGovID digital identity has been shown to be open to tax-based fraud: Curnow, "ATO."
[62]Australian Business Registry Services, "Apply for your Director ID." As demonstrated, digital identities are not *only* for end users.
[63]See World Wide Web Consortium, Verifiable Credentials Data Model v2.0.

Summary

As demonstrated throughout this article, digital identity transactions can entail complicated information flows. Privacy and security risks are posed by some of these information flows. Decentralisation generally ameliorates some of these risks by reducing the exposure of personal information. Yet this type of exposure and risk cannot be eliminated in any digital environment; by their very nature, digital transactions necessitate information.

The decentralised identity model provides selective decentralisation of certain information flows, as follows:

- It encourages direct (peer-to-peer) presentation of the identity token by the subject to the service provider without going through an identity provider at the time of a transaction. This prevents identity providers or other such parties monitoring how a subject uses their digital identity.
- It encourages specific attributes of the subject (which may or may not be identifying in themselves) to be conveyed in the form of verifiable credentials rather than general purpose identity tokens. This helps to minimise the exposure of the subject's personal information in routine transactions.
- It lessens the need for general purpose digital identity providers, which, by their nature, tend to collect larger amounts of personal information during identification to make their identity tokens more broadly useful to relying parties.

None of these architectural features are unique to the decentralised identity model. For instance, verifiable credentials are being adopted by government-operated driver's licence authorities in centralised identity environments.

The decentralisation of personal information in general should not be overestimated when consideration is given to decentralised identity. Personal information is central to many digital business transactions, such as in health care. For example, the use of decentralised identity in a patient record management system does not reduce the amount of personal data held in that system. Neither is the exposure of personal information in data breaches (such as the 2022 Optus incident in Australia)[64] necessarily a consequence of a centralised digital identity system. In the case of Optus, much of the personal information involved was identification details recorded when customers were initially identified and retained on file. A centralised identity system can be operated in a way that reduces the risk of personal information exposure by, for example, destroying identification records after the identity token is issued. Overall security and privacy risk management is affected by many implementational and operational factors and is unlikely to be determined purely by the choice of high-level digital identity management model or philosophy.

Acknowledgements
The authors are grateful to Dalvin Chien, Dr Belinda Goodenough, Associate Professor Rob Nicholls, Professor Keiran Tranter, Rachael Zavodnyik, and the anonymous peer reviewers, for their insightful and constructive comments on earlier drafts of this article. The authors are responsible for any errors in the work.

[64]Optus, **"**Optus Notifies Customers of Cyberattack."

Bibliography

Al Tamimi, Yuseff. "Human Rights and the Excess of Identity: A Legal and Theoretical Inquiry into the Notion of Identity in Strasbourg Case Law." *Social & Legal Studies* 27, no 3 (2018): 283–298. https://doi.org/10.1177/0964663917722598.

———. "Identity as Theatre? Appiah, Goffman, and the Dramaturgy of Self." *Philosophy and Public Issues* 10, no 2 (2021): 271–305.

Apple. "Apple Announces First States Signed Up to Adopt Driver's Licenses and State IDs in Apple Wallet." Press release, September 1, 2021. https://www.apple.com/newsroom/2021/09/apple-announces-first-states-to-adopt-drivers-licenses-and-state-ids-in-wallet/.

———. "macOS User Guide." Accessed October 28, 2023. https://support.apple.com/en-au/guide/mac-help/mchl4af65d1a/mac.

Australian Business Registry Services. "Apply for Your Director ID." Last modified October 12, 2023. https://www.abrs.gov.au/director-identification-number/apply-director-identification-number.

Australian Government Department of Prime Minister and Cabinet. *Connecting with Confidence*: *Optimising Australia's Digital Future. A Public Discussion Paper.* (Australian Government, 2011). https://indianstrategicknowledgeonline.com/web/connecting_with_confidence_public_discussion_paper.pdf.

Australian Government Digital Transformation Agency. *Digital Identity Legislation (a legislative framework for establishing permanent governance structures and privacy protections for the Digital Identity system) Consultation Paper.* (Australian Government, 2020). https://www.digitalidentity.gov.au/sites/default/files/2021-01/Digital-Identity-Legislation-Consultation-Paper_Accessible_131120.pdf.

Australian Securities & Investments Commission. "Director Identification Number." Last modified July 5, 2023. https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/director-identification-number.

BankID. "The Digital Card Is Here!" Accessed October 28, 2023. https://www.bankid.com/en/om-oss/nyheter/the-digital-id-card.

Bennett Moses, Lyria and Kimberlee Weatherall. "Data Problems and Legal Solutions – Some Thoughts Beyond Privacy." In *Data and the Digital Self – What the 21st Century Needs*, 18–47. Sydney: Australian Computer Society, 2023.

Boston Consulting Group and walt.id. *Me, Myself and (SS)I: Why Everybody Must Have a Self-Sovereign Identity in 5 Years*. (Boston Consulting Group and walt.id, 2021). https://web-assets.bcg.com/6b/6d/84e00cad4c939c870d833b96321c/white-paper-me-myself-ssi.pdf.

Brandler, Hannah. "Air New Zealand Launches Biometric Facial Recognition at LAX." *Business Traveller*, November 16, 2022. https://www.businesstraveller.com/business-travel/2022/11/16/air-new-zealand-launches-biometric-facial-recognition-at-lax/.

Burke, Peter and Jan Stets. *Identity Theory.* New York: Oxford University Press, 2009.

Cameron, Kim. "The Laws of Identity." *Kim Cameron's Identity Weblog: Digital Identity, Privacy and the Internet's Missing Identity Layer* (blog). May 2005. Last updated January 8, 2006. https://www.identityblog.com/?p=352.

Central IT Unit. *e-government: A Strategic Framework for Public Services in the Information Age*. (UK Cabinet Office, 2000). https://ntouk.files.wordpress.com/2015/06/e-government-strategy-2000.pdf.

Chalmers, David. *Reality+: Virtual Words and the Problems of Philosophy*. United Kingdom: Penguin, 2022.

Chesterman, Simon. *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law*. Cambridge: Cambridge University Press, 2021.

Cooper, Adam. "Eligibility and Trust in a Digital World." *The Media Bulletin*, August 30, 2021. https://www.themediabulletin.com/guest-articles/eligibility-and-trust-in-a-digital-world.

Curnow, Sarah, Dan Oakes and Kevin Nguyen. "ATO Reveals More Than $557 Million Claimed by Fraudsters Exploiting Security Loophole." *ABC News*, July 26, 2023. https://www.abc.net.au/news/2023-07-26/ato-reveals-cost-of-mygov-tax-identity-crime-fraud/102632572.

Dent, Chris. "Identity, Technology and Their Confluence: Governmentality in the Digital Age." *Law, Technology and Humans* 2, no 2 (2020): 81–96. https://doi.org/10.5204/lthj.v2i2.1437.

Diners Club International. "About Diners Club International – Join the Journey." Accessed August 24, 2023. https://www.dinersclub.com/about-us/.

FIDO Alliance. "Simpler, Stronger Authentication." Accessed October 28, 2023. https://fidoalliance.org/.

Finextra. "Westpac Backs Customer ID Management Initiative." *Finextra*, November 10, 2006. https://www.finextra.com/newsarticle/16141/westpac-backs-customer-id-management-initiative.

Goffman, Erving. *The Presentation of Self in Everyday Life.* London: Penguin Books, 1959.

Google. "Passwordless Login with Passkeys." Identity. Last modified September 12, 2023. https://developers.google.com/identity/passkeys.

Gray, Stephen and Yee-Fui Ng. "Taming the Electronic Genie: Can Law Regulate the Use of Public and Private Surveillance?" *Monash University Law Review* 48, no 3 (2023): 1–32.

Hamilton Duffy, Kim. "Decentralise What?" *O'Kims Razor – Decentralised Identity, Standards, Code, Occasionally Featuring Pugs and Cellos* (blog). December 10, 2021. https://www.okimsrazor.com/decentralize_what/.
Hendry, Justin. 'Australia's Digital Identity Bill Tops $200m', *IT News*, December 19, 2019. https://www.itnews.com.au/news/australias-digital-identity-bill-tops-200m-535700.
Jenkins, Richard. *Social Identity*. 4th ed. New York: Routledge, 2013.
Jordan, Roy. *Identity Cards and the Access Card*. (Department of Parliamentary Services, Parliament of Australia, 2006) https://parlinfo.aph.gov.au/parlInfo/download/library/prspub/3626412/upload_binary/3626412.pdf;fileType=application%2Fpdf#search=%22library/prspub/3626412%22.
Kaye, David. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. (Human Rights Council, 2015).
Kwak, Dae Hee and Sean Pradhan. " 'If You Ain't First, You're Last!' Understanding Identity Threat, Team Identification, and Advertisement Messages When Your Favourite Team Loses." *Journal of Sport Management* 35, no 2 (2021): 158–171. https://doi.org/10.1123/jsm.2019-0445.
Landau, Susan and Tyler Moore. "Economic Tussles in Federated Identity Management", *First Monday* 17, no 10 (2010). https://doi.org/10.5210/fm.v17i10.4254.
Mead, George. *Mind, Self, & Society – From the Standpoint of a Social Behaviorist*. Chicago: University of Chicago Press, 1934.
Megas, Katerina et al. *NSTIC Pilots: Catalyzing the Identity Ecosystem*. (National Institute of Standards and Technology Internal Report 8054, April 2015). https://www.nist.gov/publications/nstic-pilots-catalyzing-identity-ecosystem.
Mir, Umar Bashir, Arpan Kumar Kar and Manmohan Prasad Gupta. "Digital Identity Evaluation Framework for Social Welfare." In *Re-imagining Diffusion and Adoption of Information Technology and Systems: A Continuing Conversation*, edited by Sujeet Sharma, Yogesh Dwivedi, Bhimaraya Metri and Nripendra Rana, 401–414. International Conference on Transfer and Diffusion of IT, TDIT 2020 Tiruchirappalli, India. https://doi.org/10.1007/978-3-030-64849-7_36.
Nabben, Kelsie. "The Government Wants To Expand the 'Digital Identity' System That Lets Australians Access Services. There Are Many Potential Pitfalls." *The Conversation*, October 26, 2021. https://theconversation.com/the-government-wants-to-expand-the-digital-identity-system-that-lets-australians-access-services-there-are-many-potential-pitfalls-170550.
National Audit Office (UK). *Investigation into Verify: Report by the Comptroller and Auditor General*. (UK Cabinet Office, March 5, 2019). https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify-Summary.pdf.
National Strategy for Trusted Identities in Cyberspace. *Recommended Charter For the Identity Ecosystem Steering Group.* (US Government, National Strategy for Trusted Identities in Cyberspace, February, 2012). https://www.nist.gov/system/files/sg_draft_charter.pdf.
National Institute of Standards and Technology. *An Overview of the Fiscal Year 2012 Budget for the National Institute of Standards and Technology. Before the Committee on Science, Space, and Technology, House of Representatives, One Hundred Twelfth Congress (Hearing: March 11, 2011)*. (US Department of Commerce, April 7, 2011). https://www.nist.gov/speech-testimony/overview-fiscal-year-2012-budget-national-institute-standards-and-technology-0.
Onitiu, Daria. "Incorporating 'Fashion Identity' Into the Right to Privacy," *Law, Technology and Humans* 4, no 1 (2022): 102–116. https://doi.org/10.5204/lthj.2280.
OpenID, "Connect with Us." Accessed August 24, 2023. https://openid.net/.
Optus. "Optus Notifies Customers of Cyberattack Compromising Customer Information." September 22, 2022. https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack.
Organisation for Economic Co-operation and Development (OECD). *Digital Identity Management – Enabling Innovation and Trust in the Internet Economy.* (OECD, 2011). https://www.oecd.org/sti/ieconomy/49338380.pdf.
Puckett, Carolyn. "The Story of the Social Security Number." *Social Security Bulletin* 69, no 2 (2009): 55–74.
Ryan, Philippa. *Trust and Distrust in Digital Economies*. New York: Routledge, 2021.
Schmidt, Howard. (2011), "A National Program Office for Enhancing Online Trust and Privacy." *The White House, President Barack Obama* (blog). January 7, 2011. https://obamawhitehouse.archives.gov/blog/2011/01/07/national-program-office-enhancing-online-trust-and-privacy.
Sullivan, Clare. *Digital Identity*. Adelaide: University of Adelaide Press, 2011.
———. "Digital Identity – The Legal Person?" *Computer Law & Security Review*, 25, no 3 (2009): 227–236. https://doi.org/10.1016/j.clsr.2009.03.009.
The World Bank. *Identification for Development 2021 Annual Report*. (World Bank, 2021). https://documents1.worldbank.org/curated/en/436051643089705385/pdf/Identification-for-Development-ID4D-and-Digitalizing-G2P-Payments-G2Px-2021-Annual-Report.pdf.
———. *Identification for Development (ID4D) Global Dataset.* Data Catalog. (World Bank, 2021). https://datacatalog.worldbank.org/search/dataset/0040787.
———. *World Development Report: Digital Dividends.* (World Bank, 2016). https://www.worldbank.org/en/publication/wdr2016.

Touba, Karim. "Security Incident Update and Recommended Actions." *LastPass* (blog). March 1, 2023. https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/.
UK Government. "GOV.UK Verify is Closing." Last modified April 26, 2023. https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.
Unique Identification Authority of India. "About Aadhaar?" Government of India. https://www.uidai.gov.in/en/16-english-uk/aapka-aadhaar/14-what-is-aadhaar.html.
United Nations General Assembly. "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights." (UN General Assembly, 15 September 2021). Accessed October 31, 2023. https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021.
Wilson, Stephen. "Identities Evolve: Why Federated Identity Is Easier Said Than Done." *AusCERT 2011 Conference: "Overexposed"* Gold Coast, Australia, May 18, 2011. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2163241.
Windley, Phillip. *Digital Identity: Unmasking Identity Management Architecture (IMA)*. Sebastopol: O'Reilly, 2005.
World Health Organization. *Digital Documentation of COVID-19 Certificates: Vaccination Status: Technical Specifications and Implementation Guidance, 27 August 2021*. (World Health Organisation, 2021). https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1.
World Wide Web Consortium. "Verifiable Credentials Data Model v2.0." Accessed August 24, 2023. https://www.w3.org/TR/vc-data-model-2.0/.

Primary Legal Material

Corporations Act 2001 (Cth).
Digital Signature Act 1997 (Malaysia)
Payment Services Act (2010:751) (Sweden).
1709985 (Refugee) [2022] AATA 5089 (November 18, 2022) (Member McCulloch).
Justice K.S. Puttaswamy (Retd.) v Union of India, Supreme Court of India, Civil Original Jurisdiction, Writ Petition (Civil) No 494 of 2012 (Aug. 24, 2017).
Justice K.S. Puttaswamy (Retd.) v Union of India ('Aadhaar Case'), Supreme Court of India, Civil Original Jurisdiction, Writ Petition (Civil) No 494 of 2012 (Sept. 26, 2018).