CHAPTER

Protecting digital identity in the cloud

7

Clare Sullivan
School of Law, University of South Australia, Adelaide, Australia

1 INTRODUCTION

Technological advances have created a whole new environment for interaction. As dealings previously conducted in person are replaced by dealings without personal interaction, the requirement to provide digital identity for transactions has increased. Now digital identity is poised to assume an even greater role as governments around the world fully digitalize government services and transactions.

This is revolutionizing service delivery and the way in which government interacts and transacts with its citizens. While there are many efficiency and cost benefits, there are also significant ramifications. One of the most important ramifications is the emerging importance of digital identity.

Historically, identity has been a rather nebulous notion, especially at common law.[1] For contractual purposes, for example, identity has largely been in the background as the law focused on issues such as whether there was the necessary meeting of the minds, informed consent, and arms-length dealing. This focus, which mainly developed in response to commercial practice in the nineteenth century and early twentieth century, has led to uncertainty about the role of identity in commercial dealings.[2] Now identity, in the form of digital identity, has emerged from the shadows. While a concept of digital identity for transactions has been emergent for many years for private transactions using credit and debit cards, for example, the full implications of digital identity are now becoming apparent as governments

[1]Identity rights are generally more developed in civil law jurisdictions like France and under German and Dutch doctrine which has influenced other civil law systems such as in South Africa. Identity is recognized as an interest in personality under civil law. See, for example, in South Africa, Neethling, J., Potgeiter, J., Visser, P., 2005. Neethling's Law of Personality, 36.

[2]As one commentator observes in relation to identity, "much legal doctrine obscures the salience of identity qua identity, though when confronted directly with the issue, the law does give substance to the importance of identity." See Brookes, R.R.W., 2006. Incorporating race. Columbia Law Rev. 106, 2023–2097.

move services and transactions[3] online[4] This chapter analyzes the functions and nature of digital identity in this context, considers its vulnerability to error, and the consequences, particularly for individuals. May need to define what is digital identity in the first place.

Digital identity is an identity which is composed of information[5] stored and transmitted in digital form. Digital identity is all the information digitally recorded about an individual, i.e., a natural person that is accessible under the particular scheme. Digital identity consists of two components. The first component is a small set of defined, static information which must be presented for a transaction. Invariably, this transaction identity consists of an individual's full name, gender, date of birth, and a piece of identifying information which is typically a numerical identifier and/or a signature. The second component is a larger collection of more detailed "other information" which sits behind transaction identity in the database. This other information is updated on an on-going basis to record transaction history and can be used to profile an individual.

In many ways, transaction identity is the most important part of this digital identity because of its transactional functions which are described later in this chapter and because it is most susceptible to system error. In this chapter, system error is used in its widest sense to describe any malfunction whereby an otherwise authentic and valid digital identity is not recognized by the system.[6] This may be a spontaneous malfunction or one induced by fraud, or the malfunction may be the result of all or part of an individual's digital identity that is being used by another person. In most instances, the latter will involve dishonesty but not always.[7]

As explained in this chapter, the nature and functions of the part of digital identity required for transactions, i.e., transaction identity, mean that impact of system error on an innocent individual can be profound. This is because transaction identity directly implicates the individual linked to that identity on record, irrespective of whether or not that person actually used the digital identity to transact. Transactional rights and duties, including those arising under contract, attach to the digital identity through transaction identity. If there is subsequent default, the transacting entity will, as a matter of practicality, and arguably law,[8] look to the person linked to that identity under the scheme.

The transaction will also form part of the other information which comprises digital identity. As mentioned earlier, this other information profiles an individual. It can

[3]A transaction in this context is any dealing for which an individual is required to use digital identity. A transaction may be between an individual and a government department or agency or with a private sector entity if that is permitted under the scheme, and can range from an enquiry to a contract.
[4]Digital identity is all the information digitally recorded about an individual—i.e., a natural person—that is accessible under the particular scheme. "Information" includes "data."
[5]"Information" includes "data."
[6]This may be caused by spontaneous system failure or the malfunction may be caused by malware.
[7]The other person may use an individual's identity accidentally such as by inadvertently keying-in incorrect information, for example, though these instances would be comparatively rare.
[8]For a detailed discussion of the legal nature of transaction identity, see Sullivan, C., 2009. Digital identity—the 'legal person'? Comput. Law Secur. Rev. 25 (2), 227.

be used for both commercial and law enforcement purposes. Just as a transacting entity will look to the person linked to the identity under the scheme, so too will law enforcement authorities. As is discussed below, system error can result in a spurious record and that record can affect an individual's ability to transact under the scheme and it can have serious and long-term impact, affecting reputation and legal and commercial standing. This is more than just a remote possibility. It is a direct consequence of the architecture of the types of the scheme.

By requiring that an individual have a digital identity to transact, obviating the need for personal interaction and by automating transactions, these schemes establish a revolutionary means of transacting. They herald a new era of digital citizenship but in doing so that fundamentally change the balance of responsibility and accountability between government and citizens. Individuals, the most vulnerable sector with comparably less access to resources and information, are most affected when the system does not operate as intended.

Section 2 examines this digital identity, its functions, and its implications especially for individuals in the context of cloud computing as governments increase their use of, and reliance on, the cloud.

This development highlights the need for more effective regulation of cross-border data so the following sections of the chapter examine this emerging issue, particularly whether the focus should be on regulating cross-border data disclosure, rather than data transfer. Internationally, cross-border data protection, including the new proposal for the European Union (EU), continues to regulate cross-border data transfer, whereas the new Australia approach now regulates cross-border data disclosure. Sections 3 and 4 examine the international approach which in this respect is also supported by the United States and Asia Pacific Economic Cooperation (APEC), and compares it to the Australian regime in its ability to protect the integrity of an individual's digital identity.

May need to streamline and bring into sharper focus what is it that you want to explore and want to write about—too many themes in the introduction.

2 THE RISE OF DIGITAL IDENTITY

A specific digital identity is now emerging as governments around the world[9] move their services and transactions online. This digital identity is the primary means by which a natural person can access these services which range from social security benefits and health care to tax filing.[10] Example of what kind of information stored is important to illustrate the concept.

[9]The new scheme being rolled out in India is the most recent example of a comprehensive scheme. See IGovernment. India plans multi-purpose national ID card for citizens. igovernment.in, August 24, 2013.

[10]This chapter focuses on the consequences for individuals, i.e., natural persons.

Of the countries which are incrementally implementing these schemes, Australia is notable for its candor. The Australian government has now unequivocally stated that Australia is moving to what it calls "digital citizenship."[11] In a Discussion e-Paper released in 2011, the Australian Government acknowledges the importance of digital identity and the significant implications in the event of it being compromised:

> *In an era where our online identity is central to accessing information and services, ensuring the integrity of that identity is increasingly important. The loss or compromise of our online identity can have wide-ranging implications, including financial loss, emotional distress and reputational damage*[12]

Significantly, the paper also states that:

> *. . . there would be value in revisiting the distribution of responsibility among individuals, businesses and governments. . .Developing a common understanding of a model of accountable and responsible digital citizenship—a digital social contract—may need to be part of the debate about Australia's digital future.*[13]

In many countries, digital identity will soon be the primary means of access as government services are progressively moved online and into a digital format. There is a general requirement to use digital identity to access government services.[14] What is the linkage for this paragraph to the below?

The digital identity schemes used by governments around the world are necessarily based on the premise of one person: one digital identity. This alone is a major change, especially for common law jurisdictions in which identity traditionally has not been recognized as a distinct legal concept. How about electronic transactions in countries like Singapore under the common law? In fact, the government e-service has been ranked ahead of United States—read the Electronic Transactions Act (ETA) of Singapore to see how they handle as we are a common law country. Historically, there has been no general requirement for one legal identity. One person: one identity

---

[11] *Ibid*. The scheme is now well underway, its foundations being laid primarily through Medicare, the national health care scheme which covers all registered Australians and eligible residents. In June 2010, e.g., the Coalition supported the Labor government's proposal to compulsorily assign (with some minor exceptions) a 16-digit individual identifier to every Australian resident on the Medicare database on July 1, 2010. In relation to this Australian Individual Healthcare Identifier (IHI) which has been assigned to Australians, see the Office of the Privacy Commissioner, privacy.gov.au, September 11, 2010.

[12] *Ibid*,10.

[13] *Ibid*.

[14] While it may seem that it is still possible for an individual to transact outside the new digital system, that is generally not the case. For example, during the current transition phase, a paper tax return can still be lodged in Australia rather than using the e-filing portal. However, this is illusory. All data must now be entered into, and processed by, the digital system. If a paper tax return is filed, the information on the document is scanned into, and processed by, the digital system.

has also not been an essential commercial requirement. It has not been a requirement of private schemes like Visa credit and debit card transactions,[15] for example. For a government scheme, however, it is essential. Digitalization of government services and transactions is driven by the need to reduce costs and to increase efficiency in service delivery but most importantly, by the need to reduce fraud. A government scheme requires uniqueness and exclusivity. Consequently, an individual can legitimately have only one digital identity under this type of scheme.

The digital identity used for government services will likely set the standard for transactions with the private sector. That has been the experience internationally in the advanced digital economy of Estonia for example, and it is an outcome which is probably inevitable from a practical point of view.[16] In effect, it means that the digital identity for government transactions is the primary means by which the individual is recognized and can enter into commercial transactions. This transition is well underway in the United States, the United Kingdom, Australia, and many Asian countries but is most advanced in Europe, with Estonia the leading example of a country in which most commercial transactions require digital identity.

2.1 COMPOSITION AND FUNCTIONS OF DIGITAL IDENTITY

Digital identity in this context has specific composition and transactional functions which make its accuracy and integrity critical.

A feature of all schemes which require digital identity for transactions is that they consist of two sets of information—a small set of defined information which must be presented for a transaction, i.e., transaction identity; and the larger collection of more detailed "other information" which is updated on an on-going basis. This architecture can be depicted diagrammatically in Figure 1).

These two sets of information collectively comprise digital identity, but they are different in composition and function.

Because of its nature and functionality transaction identity is the most important part of digital identity and it is also most vulnerable to system error as defined in this chapter. Transaction identity is comparatively static, with much of the information being established at birth.[17] It typically consists of full name, gender, date of birth,

[15]An individual may have more than one credit card with more than one transaction identity. A simple example of this is an individual who has a credit card for personal use in the name John Smith which is billed to his home address and another card even from the same credit card company for business transactions in the name of Dr. J. M. Smith billed to his work address and to which is a different customer number and PIN is assigned.

[16]This is a feature of similar schemes in other countries. It is a stated feature of the new national identity scheme being rolled out in India and it was a feature of the scheme planned for the United Kingdom which was extensively documented. See for example, United Kingdom Information Commissioner. The Identity Cards Bill–The Information Commissioner's Concerns (June 2005), ico.gov.uk, May 10, 2006.

[17]Other than in exceptional cases such as gender reassignment, for example, the information which is most commonly subject to change is surname, mainly for women in the event of marriage.

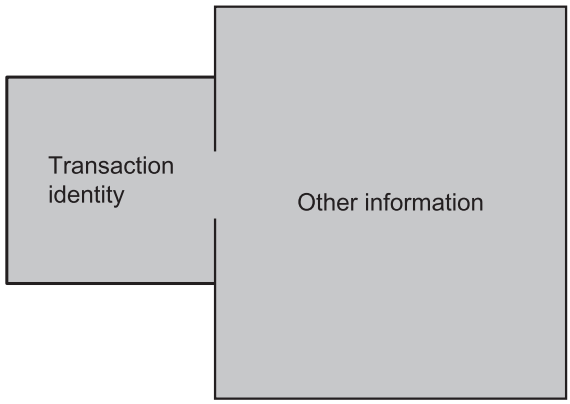

FIGURE 1

The relationship between transaction identity and the other information, which collectively make up digital identity under the scheme.

and at least one piece of what is referred to as "identifying information" which is most often a signature or numerical identifier.[18] The information which comprises transaction identity is largely public and is not of a nature which naturally seems to attract privacy protection.[19] Most significantly, transaction identity is not just information. As discussed below, it is functional.

The information which constitutes transaction identity is fundamentally different from the larger body of other information which sits behind it. That larger body of information tells a story about a person and that is its sole purpose. It is also dynamic. It is augmented on an on-going basis. Even information which at first sight seems largely administrative adds to the profile. This is also information which is not generally in the public domain. It is generally considered to be personal information which is typically protected by privacy and data protection regulation in most jurisdictions, including Australia, United Kingdom, United States of America, and in the EU. Why is this passage relevant? Access to the other information is primarily via transaction identity. The system is designed so that transaction identity is the access point and transaction identity has a gate-keeper role. Transaction identity links digital identity to an individual through the identifying information (Figure 2).[20]

These digital identity schemes depend on two processes—first, authentication of identity, and second, verification of identity. Both processes are founded on the integrity of transaction identity.

[18]In some schemes such as those in Europe and Asia, identifying information also includes biometrics, as well as a head and shoulders photograph. However, even in these schemes, biometrics is not currently required for most transactions.

[19]While being in the public domain does not necessary preclude privacy protection, the information must be of an intimate nature to attract protection. The information which constitutes transaction identity is generally not intimate in that sense.

[20]This is clear from scheme documentation. See, for example, Australian Government, Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007, 33 and 36.

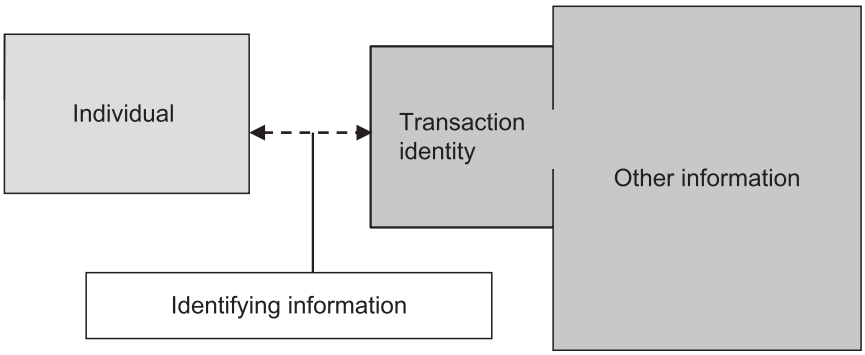

FIGURE 2

The relationship between an individual and digital identity.

The information collected when an individual is registered under the scheme is used to authenticate identity in the sense that it is used to prove authenticity. The identifying information is used to link an individual to the registered digital identity. Typically, the identifying information is a number,[21] a handwritten signature, and sometimes also a head and shoulders photo. Some schemes include biometrics as part of the identifying information. The biometrics[22] typically used are 10 fingerprints, two iris scans, and a face scan.[23] The identifying information is regarded as being associated inseparably with that individual. Once authenticated, the identity is recorded in the system.

Transaction identity, the defined, limited set of information which determines identity for transactional purposes, is then used to verify transactions.[24] Invariably, full name, gender, date of birth, and a piece of identifying information will be required to transact. Not all the recorded information need to be used for every transaction. A feature of the scheme is that the information varies, to an extent, depending on the requirements of the transacting entity. The identifying information most commonly required is a signature and/or a numerical identifier.

[21]In Australia, a 16-digit numerical identifier was assigned to every Australian resident on the Medicare database on July 1, 2010. See the Office of the Privacy Commissioner, privacy.gov.au, September 11, 2013.

[22]Depending on the nature and value of the dealing, not all or even any of these biometrics may be required for a transaction. For high level, high-value transactions, biometrics may be required as part of transaction identity but the primary role of the identifying information is to link an individual to transaction identity.

[23]Photograph is distinguished from a face scan. A face scan is a biometric. In schemes that use a face scan, the scan is not used to verify identity for all transactions. Many transactions only involve matching the appearance of the person with the photograph.

[24]Note that this is the way these terms, i.e., authentication and verification, are typically defined for the purposes of a national digital identity scheme. It is the approach used for the new Indian scheme, for example. Authentication and verification are often misused in describing the functions of transaction identity.

As a set, this information is functional in that it enables the system to transact with the identity on record. Transaction identity is verified for transactional purposes when all the required transaction information as presented, matches the information on record.[25] Transaction identity is verified by matching information with information. A human being is not central to the transaction and no human interaction is required.[26] The set of information required to establish transaction identity can be provided remotely without any human involvement at that time.

Through this matching process, transaction identity performs a number of sequential functions. First, transaction identity singles out one digital identity from all those recorded under the scheme. Second, transaction identity verifies that identity by determining whether there is a match between all the transaction identity information as presented, with that on record.[27] These two steps enable the system to recognize and then transact with that digital identity as depicted in Figure 3.

Under the scheme, there is an important distinction between identification[28] and identity. Identification is just one part of the two processes used to establish identity for a transaction. Although in some respects transaction identity may seem to replicate the traditional function of identity credentials, there is an important difference in the role played by human beings and information. Unlike traditional identity

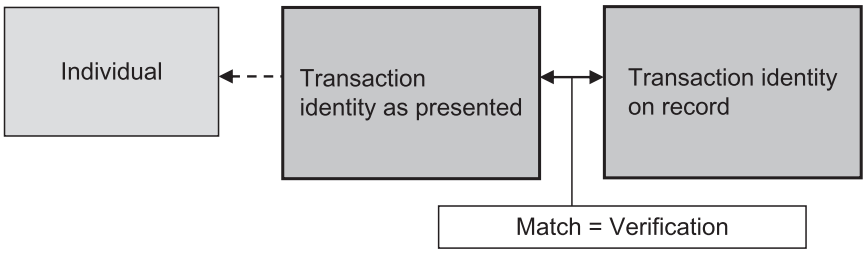

FIGURE 3

To enable transactions under the scheme, the transaction identity presented must match the identity on record.

[25]"Verify" as used in these schemes accords with its definition in the Merriam Webster Dictionary: "to establish the truth, accuracy, or reality of <verify the claim>."

[26]The set of information required to establish transaction identity can be provided remotely without any human involvement at that time.

[27]Such as name, date, and place of birth as well as with signature, photograph, and biometrics but bear in mind that not all transactions require all the identifying information. Routine transactions may only require matching photo or signature. Many low-value transactions such as those using the new Paywave technology do not require a signature or photo check.

[28]Note that separately, the information which comprises transaction identity is of limited use in identifying an individual. For example, unless it is especially unusual, name alone will not single out an individual from a population, nor will name, gender, and date of birth usually be all that is required to identify a person.

papers, the information which comprises transaction identity plays the critical role in the transaction, not the individual.[29] Digital identity does not merely support a claim to identity. Digital identity, specifically transaction identity, is the actor in the transaction. This function distinguishes transaction identity.[30]

Although the assumption is that there is a reaching behind transaction identity to deal with a person, the system does not actually operate in that way. The primary role of the identifying information is to link the registered digital identity to a person. The individual who is assumed to be represented by that identity is connected to transaction identity by the identifying information. However, this link is relatively tenuous.

A human being is not central to, or necessary, for the transaction. Transaction identity enables the transaction. The interaction is machine to machine, based on matching datasets. As a matter of fact, if not law,[31] the transaction is with the digital identity, not a person. If all the transaction identity information as presented, matches the information on record, then the system automatically authorizes dealings with that digital identity as depicted in Figure 4.

Within the scheme parameters, the system can "act and will for itself"[32] to recognize the defined set of information which comprises transaction identity and

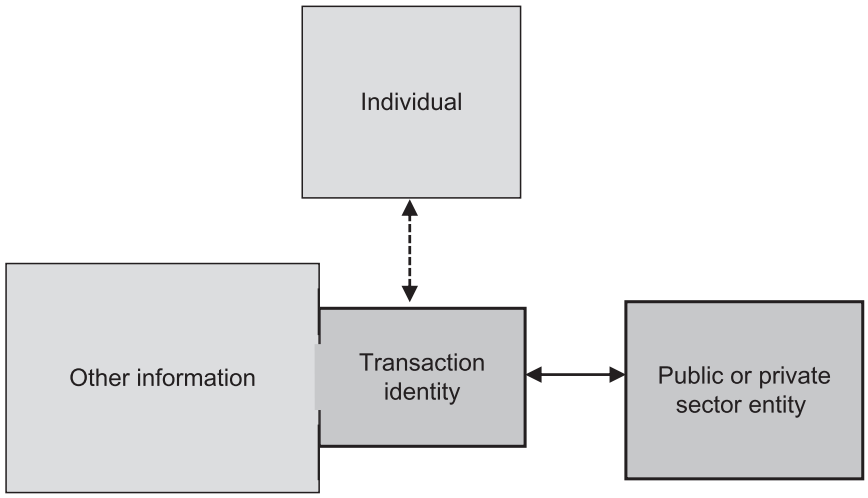

FIGURE 4

The transaction is actually with the transaction identity, not the individual.

[29]The information may be presented remotely and even automatically using computer programming, without any active involvement by an individual at the time of a transaction, though of course some human involvement is required at some stage.

[30]It distinguishes transaction identity from passports, particularly biometric passports, which are now very close to transaction identity in content, though not yet in functionality for commercial transactions.

[31]See, n 8 above.

[32]Derham, D.,1958. Theories of Legal Personality. In: Webb, L.C., (Ed.), Legal Personality and Political Pluralism, vol. 1, 14.

then transact with that identity.[33] This has significant consequences for the government as scheme administrator, for public and private sector entities using the scheme but the individual bears the most direct and significant consequences. This is because transaction identity directly implicates the individual linked to the digital identity by the identifying information,[34] and why it is important to protect the integrity of digital identity, especially now that governments are increasingly using cloud computing for their e-services and transactions. How is this link to the below passage?—sudden introduction of cloud computing?

3 THE RISE OF CLOUD COMPUTING

The cloud is now an integral part of next-generation government in many countries.[35] The widespread use of cloud computing by government and businesses has prompted the EC to describe cloud computing as providing large scale computing services as a service to the data economy in the same way as power plants supply the manufacturing industry."[36]

In essence, cloud computing is Internet-based computing. Services such as servers, storage, and applications are delivered to an organization's computers and devices through the Internet.[37] Cloud computing is commonly used to refer to

[33]The significance of this becomes evident when an otherwise legitimate digital identity is not recognized by the system. In this situation, protocol requires that the dealings be authorized with the individual, not with the digital identity. In other words, the only way to resolve the situation is to go outside the scheme.

[34]For a detailed analysis of the contractual implications, see Sullivan, C, 2012. Digital identity and mistake. Int. J. Law Inform. Technol. 20, 223–241.

[35]See, for example, in Australia, Telstra Corporation. Government: Integrated National Approach to Secure Communications. www.telstra.com.au/business-enterprise/enterprise-solutions/industries/government, September 29, 2013, where Telstra Corporation explains, "The rapid spread of digital technology and cloud computing has given government organizations an unprecedented opportunity for creating citizen-based online services, while both raising the standard of service delivery and reducing its costs. Telstra calls it "Connected Government," where government agencies at every level—federal, state, and local—are learning to be more flexible and responsive in meeting changing social and demographic dynamics. See also, Telstra Corporation. Government Blueprint Brochure. www.telstra.com.au/business-enterprise/download/document/enterprise-government-blueprint-brochure.pdf, September 29, 2013.

[36]European Commission. Communication from the Commission to the European Committee, Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions: Towards a thriving data-driven economy, SWD (2014) 214 final, 2.

[37]The generally accepted official definition of cloud computing is that of the National Institute of Standards and Technology (NIST), an agency of the US Department of Commerce published in September 2011. After, in its own words, "years in the works and 15 drafts," the final NIST definition is: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction," See National Institute of Standards and Technology. The NIST Definition of Cloud Computing. www.nist.gov/itl/csd/cloud-102511.cfm, September 24, 2013. See also the definition used by the Article 29 Working Party on the Protection of individuals with regard to the Processing of Personal Data: "[C]loud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space." See Article 29 Data Protection Working Party, "*Opinion 05/2012 on Cloud Computing*," 4.

network-based services which to the user, give the appearance of being provided by a hardware server but instead the server is simulated by software.[38] Cloud computing does away with the constraints and costs of the traditional computing environment and because of its flexibility and cost effectiveness, cloud computing has been embraced by government and businesses.

Cloud computing, by its nature, presents a significant risk to the integrity of digital identity. In its opinion on Cloud Computing adopted on 1 July 2012, the Article 29 Working Party on the Protection of individuals with regard to the Processing of Personal Data (Article 29 Working Party) highlights the range of cloud computing services[39]:

> *There is a wide gamut of services offered by cloud providers ranging from virtual processing systems (which replace and/or work alongside conventional servers under the direct control of the controller) to services supporting application development and advanced hosting, up to web-based software solutions that can replace applications conventionally installed on the personal computers of end-users. This includes text processing applications, agendas and calendars, filing systems for online document storage and outsourced email solutions.*[40]

The likelihood that the same digital identity will be used for government and private sector dealings increases the probability that it will be stored and/or processed in the cloud.

3.1 THE IMPACT OF CLOUD COMPUTING AND CROSS-BORDER DATA

Cloud computing has made data storage and access cost effective and as a consequence, it has changed the nature of cross-border data. As observed by Viviane Reding, Vice-President of the EC, EU Justice Commissioner,

> *Our world is no longer defined by physical borders. Data races from Barcelona to Bangalore. It is processed in Dublin, stored in California and accessed in Milan. In the digital age, the transfer of data to third countries has become an important part of daily life. And this affects both businesses and citizens.*[41]

[38]The Cloud is an enabler. Mobile IT, social IT, and big data, for example, are all cloud based.
[39]The Article 29 Working Party is an independent advisory body on data protection and privacy, set up under Article 29 of the *Data Protection Directive 95/46/EC*. It is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor, and the EC. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
[40]Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing, 4.
[41]Viviane Reding, Vice-President of the EC, EU Justice Commissioner Binding Corporate Rules: unleashing the potential of the digital single market and cloud computing, IAPP Europe Data Protection Congress Paris, 29 November 2011.

Data does not have to be stored or processed in another country or transferred across a national border in the traditional sense to be cross-border data. This is an important development considering the functions of transaction identity and the consequences of system error. While cloud computing has many benefits, it has inherent risks. On 1 July 2012, the Article 29 Working Party in its opinion on Cloud Computing[42] stated that,

> *Despite the acknowledged benefits of cloud computing in both economic and societal terms, . . . the wide scale deployment of cloud computing services can trigger a number of data protection risks, mainly a lack of control over personal data as well as insufficient information with regard to how, where and by whom the data is being processed/sub-processed. These risks need to be carefully assessed by public bodies and private enterprises when they are considering engaging the services of a cloud provider*[43]

The opinion lists the specific risks of personal data processing using cloud computing, in two broad categories: control and lack of transparency,

> *Lack of control*
>
> *By committing personal data to the systems managed by a cloud provider, cloud clients may no longer be in exclusive control of this data and cannot deploy the technical and organizational measures necessary to ensure the availability, integrity, confidentiality, transparency, isolation, intervenability and portability of the data.*
>
> *Lack of information on processing (transparency)*
>
> *Insufficient information about a cloud service's processing operations poses a risk to controllers as well as to data subjects because they might not be aware of potential threats and risks and thus cannot take measures they deem appropriate* [44]

These risks can undermine the integrity and functionality of digital identity. A digital identity scheme is characterized by the enduring nature of the identity information required for transactions and its unique association with that individual. The transacting entity will, as a matter of practicality, if not law, look to the person linked to that identity.

The challenge then faced by that individual can have two aspects. Difficulty can arise in that individual establishing that "I am who I say I am" and in establishing "I am not who the record says I am." This is so if the set of information which constitutes transaction identity is used by another person or if the transaction identity information is misrecorded, misread, or incorrectly linked as a result of system malfunction or fraud. Another person's signature, for example, may be being linked with the full name, gender, and date of birth of individual A. In this situation, individual A will be on record as entering into the transaction. The person identified as

[42] Above n 40, 8.
[43] Above n 40, 2.
[44] *Ibid.*

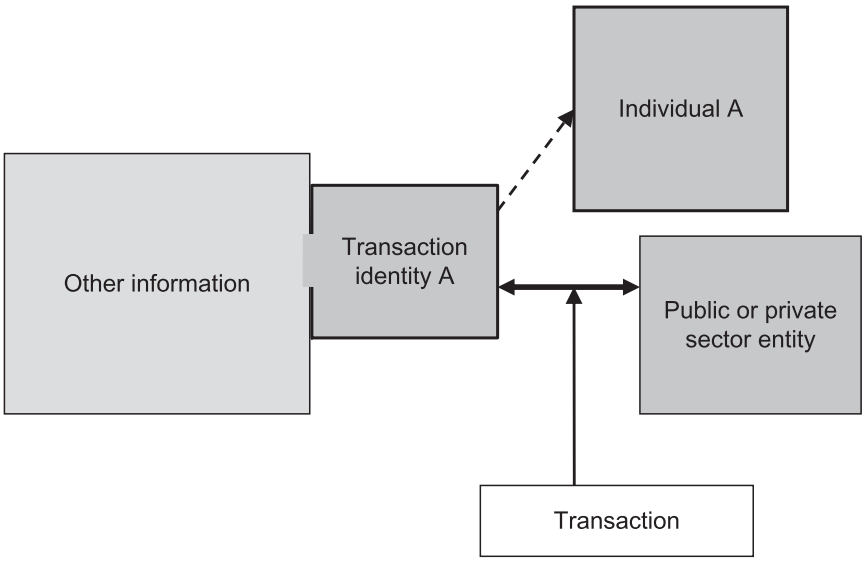

FIGURE 5

The transaction is with transaction identity A and that identity is linked to individual A.

doing the transaction is individual A and written records of the dealing will also refer to individual A as depicted in Figure 5.

This scenario illustrates the practical and legal implications for an innocent individual. Individual A must establish that he/she did not enter into the transaction and this can present significant difficulty. Considering that transactions can be conducted from anywhere in the world, 24 h a day, individual A may not be able to establish that he or she did not enter into this transaction. Individual A may not even become aware of the transaction until much later, such as when an item appears on an account or overdue notice.

The impact on the innocent individual is immediate though, even if he/she is not immediately aware of it. The other information, which makes up digital identity, records transactions on an on-going basis. That information is used to monitor and establish the basis on which an individual can continue to transact under the scheme. Protection protocols programmed into the system can cause considerable harm to an innocent individual. If wrong-doing is suspected or there are suspicions that the digital identity has been compromised, the system can automatically suspend transactions with transaction identity A. Not being able to transact under the system goes beyond frustration and inconvenience. In a world where digital identity is required for everything from employment applications and tax filing, to welfare payments and health care, being unable to use the system, even temporarily, can have major consequences.

There can be even more serious implications. The other information which makes up digital identity can also be used to profile an individual for other purposes. If, for example, transaction identity A is used by individual B to order

material which can be used for bomb making or to download bomb-making instructions, that activity can be detected through routine monitoring. It could lead to individual A being suspected of terrorist activity. The consequences for individual A can range from impact on reputation, to criminal charges, both of which can be very difficult for A to refute and defend. This scenario is far from fanciful and it is not just an unfortunate occurrence. It is a direct consequence of the scheme's design and operation.

Digital identity schemes operate on the premise that transaction identity will only be used by the person on record. Regardless of whether the error is accidental or induced by misuse, the error compromises the integrity of an individual's digital identity. The ease with which data can now be moved, processed, and accessed around the world using the cloud, heightens the concern, as the EC noted in 2013:

> *The rapid pace of technological change and globalisation have profoundly transformed the scale and way personal data is collected, accessed, used and transferred. There are several good reasons for reviewing and improving the current rules, which were adopted in 1995: the increasingly globalised nature of data flows, the fact that personal information is collected, transferred and exchanged in huge quantities, across continents and around the globe in milliseconds and the arrival of cloud computing. In particular, cloud computing—where individuals access computer resources remotely, rather than owning them locally—poses new challenges for data protection authorities, as data can and does move from one jurisdiction to another, including outside the EU, in an instant. In order to ensure a continuity of data protection, the rules need to be brought in line with technological developments*[45]

Cross-border data is currently regulated in the European Union (EU) under the Data Protection Directive 95/46 EU of the European Parliament and of the European Council of 24 October 1995 (Directive).The Directive protects EU citizens in relation to processing of their personal data and the movement of that data,[46] and covers the use of cloud computing services.[47]

Article 25.1 of the Directive prohibits the transfer of personal data to a third county (i.e., a country or territory outside the European Economic Area (EEA)) unless that third country provides an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. An organization is prohibited from transferring data about EU citizens, whether they

[45]EC. How Will the EU's Reform Adapt Data Protection Rules to New Technological Developments? 1 ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf, September 29, 2013.

[46]The reference to data is of no consequence because the definitions under the Directive and the Australian Privacy Act include both data and information.

[47]This is confirmed by the Article 29 Working Party in its opinion on cloud computing. In that opinion, the Article 29 Working Party also confirmed that the e-privacy Directive 2002/58/EC (as revised by 2009/136/EC) also applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks (telecom operators) and is relevant if those services are provided by means of a cloud solution. See above n 40, 6.

are employees, customers, or other contacts, unless there is compliance with Article 25. This means that organizations are prohibited from sending personal information outside the EEA except where adequate protections have been put in place, or where the destination country has been pre-approved as having adequate data protection.

Data transfers to third countries can occur in many circumstances, such as where an EU-based business relocates functions to subsidiaries outside the EEA, establishes an offshore shared service center which processes HR or payroll data, for example, hosts offshore and/or processes data as part of an outsourcing agreement with a third-party supplier or uses cloud computing. The onus is on the data controller to ensure that there is compliance with the 8th data protection principle in relation to any cross-border data transfer of personal data.

In January 2012, the EC proposed "comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy through a global standard[48]:

> "*. . ..the Commission is proposing a system which will ensure a level of protection for data transferred out of the EU similar to that within the EU. This will include clear rules defining when EU law is applicable to companies or organisations established outside the EU, in particular by clarifying that whenever the organisation's activities are related to the offering of goods or services to EU individuals or to the monitoring of their behaviour, EU rules will apply. The Commission is proposing a streamlined procedure for so-called "adequacy decisions" that will allow the free flow of information between the EU and non-EU countries. An adequacy decision is an acknowledgement that a given non-EU country ensures an adequate level of data protection through its domestic law or international commitments. Such adequacy decisions will be taken at European level on the basis of explicit criteria which will also apply to police cooperation and criminal justice.*
>
> *Businesses operating globally will benefit from clear and explicit rules for making use of binding corporate rules, as well as from the fact that prior authorisation will no longer be needed for transfers covered by binding corporate rules or standard contractual clauses. The proposal will promote effective international cooperation for data protection enforcement between the Commission, European data protection authorities and authorities outside the EU, through investigative assistance, information exchange and complaint referral. Lastly, by promoting global standards, the Commission's proposals will ensure continued European leadership in protecting data flows around the world.*"[49]

[48]EC. Commission Proposes a Comprehensive Reform of the Data Protection Rules, Brussels, January 25, 2012. ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm, September 29, 2013. See also, EC. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (25 January 2012). ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, September 29, 2013.

[49]EC. How will the EU's Data Protection Reform Simplify the Existing Rules?. ec.europa.eu/justice/data-protection/index_en.htm, September 29, 2013.

The key changes proposed by the Commission are:

- "Clear rules on when EU law applies to data controllers outside the EU, in particular, by specifying that whenever controller's activities are related to the offering of goods or services to EU individuals, or to the monitoring of their behavior, EU rules will apply.
- Streamlined adequacy decisions that allow free flow of information between the EU and non-member countries taken at European level on the basis of explicit criteria, and which will also apply to police cooperation and criminal justice.
- Making legitimate transfers easier and less burdensome by reinforcing and simplifying other rules on international transfers, in particular by:

  Streamlining and extending the use of tools such as 'binding corporate rules',[50] so that they can be used to also cover data processors and within 'groups of companies', thus better reflecting the multiplicity of actors involved in data processing activities especially in the framework of cloud computing."[51]

In effect, the proposed regulation will establish a single European law for data protection, replacing the current inconsistent patchwork of national laws. The hope is that increased harmonization will be achieved by having a single set of rules applicable across the EU and a "one-stop-shop" enforcement system, whereby a single data protection authority is responsible for an organization operating in several countries. The example given by the Commission is of a chain of shops which "has its head office in France and franchised shops in 14 other EU countries. Each shop collects data relating to clients and transfers it to the head office in France for further processing. Under current rules, France's data protection laws would apply to the processing done by head office, but individual shops would still have to report to their national data protection authority, to confirm they were processing data in accordance with national laws in the country where they were located."[52] The responsible authority will be the data protection authority in the organization's home base. Each business will be answerable to only one data protection authority, and both businesses and consumers will have a single point of contact.

[50]The EC explains, "Binding corporate rules are one tool that can be used to adequately protect personal data when it is transferred or processed outside the EU. Businesses can adopt these rules voluntarily and they can be used for transfers of data between companies that are part of the same corporate group. Currently, in order to be approved, binding corporate rules must be verified by at least three data protection authorities" See, EC. "How Will the EU's Data Protection Reform Make International Cooperation Easier?. ec.europa.eu/justice/data-protection/index_en.htm, September 29, 2013. The current major data transfer schemes are the EU's Binding Corporate Rules framework (BCR) and the Asia Pacific Economic Cooperation's (APEC's) Cross Border Privacy Rules System (CBPR) which are under review and following similar approach to that proposed by the EC.

[51]*Ibid.*

[52]See, above n 48.

Most importantly, under this proposal, companies based outside the EU will have to abide the same rules as European companies. The stated objective is to protect EU citizens' data throughout the world:

> *When the EU cooperates with non-member countries, the Commission's proposals will make sure that citizens' data is protected throughout the world, and not only within the EU. This will help to improve international trust in the protection of individuals' personal data, wherever the data is located. This will in turn promote growth opportunities for EU businesses. EU data protection standards have to apply independently of the location where the data relating to EU individuals is processed. At the same time, data transferred outside the EU should be protected. Businesses committed to a high level of data protection should be provided with simple tools to ease legitimate transfers. Third party cooperation on these new proposals will help to ensure that Europeans' personal information is safe wherever it is in the world.*[53]

European regulators will have strong enforcement powers. Data protection authorities will be able to fine companies who do not comply up to 2% of their global annual turnover.

On March 12, 2014, this reform was strongly endorsed by the European Parliament. This is a significant development which indicates that this reform will proceed to a Regulation of general application to members of the European Union.[54]

The EC proposal is therefore the most important international development in terms of its international application and its influence. Similar cross-border data protection proposals have also been advanced by the United States and by APEC. While there are presently some differences in approach that are likely to be resolved soon, there is broad international agreement on the need to harmonize the major data protection regimes, especially as they apply to cross-border data[55] and for a new global standard.

The key point, however, is that by framing regulation in terms of transfer, all these proposals fail to address full the impact of cloud computing and the risks it entails, especially to digital identity. Transaction identity is required for processing transactions so it is disclosed when dealing with overseas call centers, for example, even if it is not actually transferred across a border. Yet the notion of physical borders and transfers still pervades these proposals for reform.

---

[53] *Ibid.*

[54] With 621 votes in favor, 10 against and 22 abstentions for the Regulation; and 371 votes in favor, 276 against and 30 abstentions for the Directive, providing an important signal of support in the legislative process. See, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote, Strasbourg, March 12, 2014.

[55] This point has been made by the United States' Federal Trade Commission: "[e]fforts underway around the world to re-examine current approaches to protecting consumer privacy indicate an interest in convergence on overarching principles and a desire to develop greater interoperability." See FTC Report. *Protecting consumer privacy in an era of rapid change*, March 2012, 10.

The notable exception is Australia which in the 2013 reforms to the Privacy Act 1988 (Cth) (Privacy Act) moved from regulating transfer of cross-border data to regulating disclosure.

What is the relevance of EU in this whole scheme?

4 PROTECTING DIGITAL IDENTITY IN THE ERA OF CLOUD COMPUTING

In 2012, the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) (Reform Act) was passed by the Australian federal Parliament. The Reform Act was the culmination of a comprehensive privacy law reform process which began almost 20 years after the Privacy Act was first introduced in 1988.[56] Most of the changes came into operation on 12 March 2014.[57]

Until the enactment of the Reform Act, the Australian Privacy Commissioner's role was largely one of monitoring and conciliation, with some power to investigate and take action in respect of clear breach of the Privacy Act. Under the new regime, Australia has moved to a stronger regulatory scheme with greater powers given to the Commissioner. Most significant, however, is Australia's new approach in regulating cross-border disclosure.

The Reform Act continues to permit the collection, use, and disclosure of personal information with consent but creates a new set of "Australian Privacy Principles" (APPs) that apply to both government agencies and private sector entities.[58] The APPs echo the earlier privacy principles in many respects but are structured differently, stepping through the data-handling process from the stage of planning the collection of personal information, collecting the information, using and handling it, and finally

[56]On January 31, 2006, the Australian Law Reform Commission (ALRC) received Terms of Reference from the Australian Attorney-General for an inquiry into the extent to which the Privacy Act 1988 (Cth) and related laws continue to provide an effective framework for the protection of privacy in Australia. The changes made by the Reform Act implement the Australian Government's first-stage response to the ALRC's Report 108: *For Your Information: Australian Privacy Law and Practice*. Some notable reforms recommended by the ALRC have not yet been enacted. These recommendations include proposals to remove certain exceptions such as the small business exception, make data breach notification mandatory, and to introduce a statutory cause of action for interference with an individual's privacy. However, the Government has expressed an intention to deal with these in a second stage of reforms.

[57]The Privacy Amendment (Enhancing Privacy Protection) Act 2012 was passed by federal Parliament on 29 November 29, 2012 and received royal assent on December 12, 2012. The majority of the amendments take effect in March 2014, though a handful of provisions apply from the date of royal assent, i.e., December 12, 2012.

[58]Previously, there were two sets of principles, one for government and the other for business, though they were very similar. This reflected the Act's evolution. Initially, the legislation applied only to government. The Act was later amended to apply to the private sector. The Act now defines "entity" to mean: "(a) an agency; or (b) an organization; or (c) a small business operator." See section 6(1) Privacy Act.

disposing of it. Generally, the APPs have a greater emphasis on open and transparent management of personal information.

A number of APPs introduce significant change,[59] the most notable of which is the new APP 8 which with section 16C regulates cross-border disclosure of information. APP 8.1 introduces a new accountability approach to cross-border disclosure of personal information which fundamentally changes the previous liability regime regulating transfer of personal information to recipients outside Australia. The main reason for the change seems to be to deal with temporary transfers such as those often used for e-mail routing which were the discussed in the report of the Australian Law Reform Commission which prompted reform of the Privacy Act.[60] However, the change to disclosure is a major reform which has far reaching implications, especially now that the cloud is now an integral part of next-generation government.[61] The Senate Report notes that the use of the term disclosure creates more clarity than transfer:

> *the ordinary meaning of disclosure is to allow information to be seen rather than the implication of 'transfer' of a cross-border movement of information. This means that a disclosure will occur when an overseas recipient accesses information, whether or not the personal information that is accessed is stored in Australia or elsewhere.*[62]

[59]Significant amendments which can be relevant to the other information which comprises digital identity are made to the credit reporting scheme through new rules that regulate information disclosed to and by credit reporting bodies, credit providers, and other information recipients. The new rules for credit reporting bodies and credit providers balance the protection afforded to the individual and the credit provider's access to reliable credit information about an individual. Disclosure of repayment history is permitted in certain instances from the date of assent. The disclosure of this historical data allows the credit reporting system to play a more meaningful role in assessing an individual's credit worthiness from commencement. Civil penalties replace the majority of the criminal offences with respect to noncompliance with the new rules, however, criminal offence provisions still apply with respect to false and misleading information. Civil penalties of up to $1.1 million can be sought by the Commissioner for breaches of credit reporting requirements.

[60]ALRC. Review of Australian Privacy Law, DP 72 (2007), Question 28–1. The impact of the Internet on privacy is discussed in Chapters 9 and 11.

[61] Telstra Corporation. *Government: Integrated National Approach to Secure Communications*. www.telstra.com.au/business-enterprise/enterprise-solutions/industries/government, September 29, 2013 where Telstra Corporation explains, "The rapid spread of digital technology and cloud computing has given government organizations an unprecedented opportunity for creating citizen-based online services, while both raising the standard of service delivery and reducing its costs. . . ..Telstra calls it "Connected Government," where government agencies at every level—federal, state, and local—are learning to be more flexible and responsive in meeting changing social and demographic dynamics. See also, Telstra Corporation. Government Blueprint Brochure. www.telstra.com.au/business-enterprise/download/document/enterprise-government-blueprint-brochure.pdf, September 29, 2013.

[62]*Senate Finance and Public Administration Committees*, *Parliament* of Australia, Senate, *Exposure Drafts of Australian Privacy Amendment Legislation Report Part 1–Australian Privacy Principles* (2011), http://www.aph.gov.au/~/media/wopapub/senate/committee/fapa_ctte/completed_inquiries/2010-13/priv_exp_drafts/report_part1/report.ashx, para 11.47, October 17, 2012.

By regulating disclosure,[63] rather than transfer, the scope of APP 8 is broadened both in the activities it covers and the entities to which it applies. Increasing use of technology-related services which involve immediate exchange of information through global telecommunications networks and cloud computing means that most entities are more likely to be involved in disclosure of personal information to overseas recipients. Under APP 8, an entity may disclose personal information to an overseas recipient, provided it takes such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to that information. However, even where the entity does so, the entity will, in certain circumstances, be deemed to be liable for any subsequent breaches of the Privacy Act committed by the overseas recipient. The only way an entity can escape the effect of this deeming provision is to rely on one of the relatively narrow exceptions now specified in the Act which in summary, are where there is:

1. Reasonable belief by the entity that:
   - **(i)** the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information; and
   - **(ii)** there are mechanisms that the individual can access to enforce the protection of that law or binding scheme

   or
2. Consent by the Individual
   The individual consents to disclosure of the information after being expressly informed by the entity that if the individual consents to the disclosure of the information, the requirement to take reasonable steps will not apply to that disclosure.
   or
3. Information disclosure compelled by law
   - where the cross-border disclosure is required or authorized by or under an Australian law, or a court/tribunal order (APP 8.2(c))
   - where an organization reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (APP 8.2(d), s16A item 1)
   - where an organization reasonably believes that the disclosure is necessary to take action in relation to the suspicion of unlawful activity or misconduct of a serious nature that relates to the organization's functions or activities (APP 8.2(d), s 16A item 2)

[63]Disclosure lies at the heart of the right to privacy. This is so in relation to the right to privacy under the *European Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature November 4, 1950) 213 UNTS 221, which is the basis for privacy protection in Europe and which is influencing the development of privacy in Australia, and it is also so for the right to privacy under US law.

- where an organization reasonably believes that the disclosure is necessary to assist any entity, body, or person to locate a person who has been reported as missing (APP 8.2(d), s 16A item 3).

The new APP 8 has a number of significant ramifications for Australian organizations. APP 8 applies to all offshore outsourcing including offshore call centers, offshore data hosting, and/or processing services, and cloud computing generally where there is access to information. Deemed liability under APP 8 and the new penalties and powers of the Commissioner significantly increase the risk of liability. Where entities are unable to rely on the consent or reasonable belief exceptions, they can potentially be held liable for serious or repeated breaches of privacy by the overseas recipient. Entities covered by the Act[64] which handle personal information must ensure that their privacy policies and procedures comply with the new privacy principles.

Any disclosure of personal information must comply. There are no "saving provisions" for disclosures made under existing contracts. Entities will have to check that their existing and planned offshoring arrangements and cloud computing contracts comply with the new requirements. In effect this means that entities have to manage the risk they face through a combination of technical measures and provisions in their contracts with the overseas entities.

Most significantly, by regulating cross-border disclosure, APP 8 applies to offshoring arrangements which were established on the basis of no transfer of personal information. Even if the information remains in Australia, APP 8 applies provided there is disclosure to a party offshore. This is an important step in increasing protection of all the information which comprises digital identity but especially for increasing protection for transaction identity.

5 CONCLUSION

Digital identity schemes are now part of life in many countries and are set to become the norm as more governments digitalize services and transactions. What sets this type of scheme apart is the impact of system error on the individual. This is because the digital identity required for transactions is now the primary means by which a person is able to operate in this new virtual world.

The scheme is also characterized by the enduring nature of the identity information required for transactions and its unique association with an individual. These two essential features result in practical and legal issues for that individual when system does not correctly recognize the identity or when it permits the identity to

[64]The Act applies to individuals, bodies corporate, partnerships, unincorporated associations, and trusts. There is an exemption for small business. See section 6 C Privacy Act. A business is a small business at a time (the test time) in a financial year (the current year) if its annual turnover for the previous financial year is $3,000,000 or less. See section 6 D Privacy Act.

be misused by another person. Regardless of whether it is spontaneous or is induced, the error compromises the integrity of an individual's digital identity.

Offshore storage, hosting, and processing, especially in the cloud, increases the risk of compromise. The EU, United States, and regional bodies are working to address the challenges presented by technology and all seek to address the shortcomings of the present piecemeal approach. There are clear benefits for individuals and organizations in streamlining compliance. The EC's view is that "new simpler, clearer and stronger rules will make it easier for citizens to protect their data online. They will also cut costs for business considerably, providing EU companies with an advantage in global competition, as they will be able to offer their customers assurances of strong data protection whilst operating in a simpler regulatory environment."[65] There is, however, an important distinction between data transfer and disclosure which has been overlooked in the proposals of the EU, United States, and APEC.

With the advent of cloud computing there may not be a transfer of data across a border but there can be disclosure. In recognizing that disclosure is the now key issue, the Australian approach is a preferable model. APP 8 provides much needed additional protection to an individual's personal information in a contemporary environment which is characterized by the growing significance of digital identity and the increasing use of cloud computing. In line with the Australian government's statement about developing a model of accountable and responsible digital citizenship, APP 8 clearly signals that it is important for both government and private sector entities to be aware of when and how personal information is disclosed. APP8 requires that the entity obtain individual consent after having clearly and unambiguously set out how at the information is or may be disclosed. In the absence of that consent, the entity must ensure that information is protected to the same standard as it would be in Australia.

This level of specificity is necessary to alert individuals to their rights, and in the case of government and private sector entities, to make them fully aware of their data-handling responsibilities. This awareness of rights and responsibilities is more important than ever, at a time when an individual's ability to transact increasingly depends on the integrity and functionality of digital identity.

The whole essay seems to be a description of various schemes without any unifying focus—pretty confusing about what the author is trying to say—lack of in-depth treatment or analysis and not quite sure what is the problem the author is trying to solve or described. More of a survey—overview.

[65]EC. ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-14, September 29, 2013.