

# **Digital Citizenship: Digital Identity, Right to Privacy, and the Right to Identity in the United States of America**

Dr Clare Sullivan.

South Australian Fulbright Scholar 2011/12, Lecturer, School of Law University of South Australia Campus West, George Street, Adelaide South Australia 5000, Australia. Research Fellow, Law School, Ligertwood Building, North Terrace, Adelaide SA 5005, Australia. Telephone: 61 8 803020308. Email: clare.sullivan@unisa.edu.au

This paper was written while Dr Sullivan was Visiting Scholar at the Law School, George Washington University, Washington DC. An earlier version of the paper was presented at the Privacy Scholars Conference in Washington DC in June 2012.

## **Abstract**

This paper examines the relationship between digital identity, the right to privacy at common law and under legislation and the right to identity in the United States.

The paper focusses on a government scheme which requires that an individual establish his or her digital identity for transactions. These schemes are being established by many governments around the world but this paper examines the situation in the United States of America at federal level. The approach in the United States, is compared with international developments especially those in Australia. Australia has taken similar implementation steps to the United States and has recently announced the need to review the distribution of responsibility among individuals, businesses and governments, as a consequence of this move to “digital citizenship.”

The functions and legal nature of digital identity are examined in the context of a federal scheme in the United States. The implications for individuals, government agencies and the private sector are considered, particularly in the context of system malfunction and identity theft and fraud.

While an individual has a natural interest in protecting his or her digital identity, the accuracy and integrity of the registered identity also underpins the integrity of the scheme. The ability of privacy, at common law, under legislation and under the proposed Consumer Privacy Bill of Rights, to protect digital identity is compared and contrasted to the protection provided by another comparatively neglected right, the right to identity.

While the right to privacy provides general protection to digital identity, by its nature privacy does not adequately protect the part which is required for transactions. The right to identity however can protect transaction identity. The right to identity, like the right to privacy, can, and should, be recognized in the United States as an integral part of the move to digitalize government services.

Keywords: Digital identity, transactional identity, right to privacy, right to identity, United States of America.

## **Introduction**

A concept of digital identity for transactions has been evident in commercial practice for many years. However, the full implications of this development are now emerging as governments digitalize government services. This initiative is driven by the need to reduce costs, to increase efficiency in service delivery, and most importantly, to reduce welfare fraud. Consequently, the premise of one person: one identity is an essential feature of these government schemes.

This is a significant development because historically identity has a nebulous concept. Identity has largely been in the background in commercial transactions, resulting in uncertainty about its legal role and nature in a

transactional context, especially at common law.<sup>1</sup> The move to digitize government services and transactions between individuals and government agencies elevates digital identity to a new level of commercial and legal significance.

There are also broader ramifications. Although one person: one identity has not been an essential requirement for private schemes like Visa credit and debit card transactions for example,<sup>2</sup> the digital identity recognized by the government has implications for all schemes which use digital identity for transactions because it can set the standard for private sector dealings.<sup>3</sup>

These factors make analysis of the functions and legal nature of digital identity in a transactional context important and timely. To date, privacy has been the primary focus of legal scholars and the courts and there is an extensive body of international legal scholarship on protection of personal information. However, as the analysis in this paper shows, an individual's digital identity, particularly the set of information required for transactions, is more than just personal information. Its functions under the scheme give it specific legal character.

This paper analyzes the functions, and legal nature, of an individual's digital identity in the context of a federal government scheme. The analysis sets out the implications for individuals, government and the private sector. In the light of these implications, the protection provided by privacy in the United States is compared to the right to identity, an international human right, the importance of which has been largely obscured by the focus on the right to privacy.

There are several neglected questions which are considered: How does the right to identity differ from the right to privacy? Does the right to privacy protect digital identity? In particular, how do the right to privacy and the right to identity relate to the concept of digital identity? This paper examines these questions in the context of United States' federal law.

## **The Approach of the Paper**

The paper begins by considering digital identity as an emergent legal concept. Digital identity is an individual's identity which is composed of information<sup>4</sup> stored and transmitted in digital form. Digital identity is all the information digitally recorded about an individual<sup>5</sup> which is accessible under the particular government scheme.

In all schemes which require that an individual establish his or her digital identity to transact, the identity information is invariably divided into two groups - a small set of defined information which is must be presented for a transaction and a larger collection of information which is broader information such as transaction history. This other information is more detailed and dynamic because it is updated on an on-going basis. Collectively, this other information, and the smaller set of information which is an individual's transaction identity, constitutes an individual's digital identity under the scheme.

Transaction identity is the most significant part of digital identity in terms of its functions and its implications. Transaction identity consists of a small group of relatively static information, typically full name, gender, date of birth and at least one piece of identifying information such as a signature. Separately this information is of comparatively little use or consequence. As a set, however, it enables transactions under the scheme. While the larger set of information which makes up digital identity is essentially personal information, transaction identity

---

<sup>1</sup> Contract law, for example, generally focuses on agreement and whether the transaction is 'at arms-length' and the parties are usually assumed to be indifferent to each other's identity. 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 Richard R.W. Brookes "Incorporating Race" (2006) 106 *Columbia Law Review*, 2023, 2097.

<sup>2</sup> 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.

<sup>3</sup> This is a stated objective of many national identity schemes but even if it is not an objective, it is an outcome which is almost inevitable.

<sup>4</sup> 'Information' includes 'data.'

<sup>5</sup> 'Individual' is a natural person who has been born, irrespective of whether or not the person is currently alive or is deceased.'

is more than just personal information. It has a role as gatekeeper to the larger body of other information and it has specific functions at the time of a transaction which arguably give transaction identity specific legal character.

Transaction identity is the most significant part of digital identity to an individual. The accuracy and functionality of transaction identity is also important to government agencies using the scheme and to the government as scheme administrator. This is because of the nature and functions of transaction identity. As a set, the information which constitutes an individual's transaction identity takes on a different legal character. Its components are transformed from personal information, into a collective which has legal personality, and which gives rise to specific rights and liabilities. This paper argues that because of the significance of transaction identity and its consequences for an individual and for the overall integrity of the scheme, transaction identity requires greater protection than can be provided by the right to privacy.

The central argument presented in this paper is that privacy protects all of the information which comprises an individual's digital identity under the scheme because it is personal information. However, by its nature, privacy is not capable of providing adequate and appropriate protection to transaction identity. The right to identity can provide the protection required because it is a more robust right than the right to privacy. Both these rights are needed to adequately protect digital identity but the right to identity has been largely overlooked in the United States because of the focus on privacy.

Although they are closely related and often overlap, the right to identity and the right to privacy are separate and distinct legal rights. Both relate to individual autonomy but the right to identity and the right to privacy protect different interests in different ways. This paper examines the basic differences and the implications for digital identity and particularly for transaction identity.

The argument that privacy is not capable of providing adequate and appropriate protection to transaction identity applies irrespective of whether it is the right to privacy at common law, as prescribed under legislation or as proposed in the Consumer Privacy Bill of Rights.<sup>6</sup> Consequently because the analysis focusses on the essence of privacy, in this paper, the right to privacy encompasses the Constitutional right to privacy and privacy rights recognized and protected under federal and state privacy legislation, unless otherwise indicated.

Recognition of the right to identity in the United States would strengthen the protection currently available under the right to privacy. The right to identity can be recognized and protected through statute as part of a suite of legislative protections which include privacy. There is also scope for judicial recognition of the right to identity in much the same way as the courts have recognized and developed the right to privacy in response to need in changing times. The paper concludes by outlining an argument along similar lines to the reasoning followed in recognizing the right to privacy.

The analysis in the paper shows that in the context of a government scheme, the right to identity takes specific form as the right to an accurate, functional transaction identity. This right can, and should, be recognized in the United States as an important part of the move to digitalize government services.

## **Digital Identity in the United States**

The emergence of digital identity as a new legal concept is especially clear in the context of a formal national identity scheme such as those in Europe and Asia.<sup>7</sup> Earlier scholarship argues that digital identity emerged as a distinct new legal concept in the United Kingdom in 2006 as a consequence of that country's scheme. The United Kingdom scheme has since been largely dismantled but it is still representative of contemporary schemes in Europe and Asia.<sup>8</sup> The United Kingdom scheme was based on earlier schemes in Europe, most notably the Belgium scheme, and is the model for the new scheme planned for India.<sup>9</sup>

---

<sup>6</sup> *Consumer Data Privacy in a Networked World. A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, The White House, February 2012.

<sup>7</sup> The most recent example in Asia is the national identity scheme being introduced into India. See, IGovernment, '*India plans multi-purpose national ID card for citizens*' <igovernment.in> at 24 August 2010. In Europe the most recent example is the new E- tax card in Greece.

<sup>8</sup> Clare Sullivan, Digital Identity, 2010. See also Clare Sullivan, 'Is Your Transaction Identity Property?' paper presented at the 2012 Property, Law and Society WIP, Georgetown University; Clare Sullivan, Digital Identity and Privacy, Internet WIP, New York University; Clare Sullivan, 'Digital Identity – The "Legal Person"?' (2009) 25(2) Computer Law and Security Law Review 227; Clare Sullivan, 'Is Identity Theft Really Theft?' (2009) 23(1-2) International Review of Law,

These schemes are rolled out nationally, usually with considerable fanfare. They are established by specific legislation, although it is important to note that the legal character of digital identity arises from scheme operations, rather than through specific legislative statement. This point is important in the context of the United States because such a scheme can be established gradually through incremental change.

The United States and other countries, most notably for this paper, Australia have adopted the more subtle approach. Although the schemes being implemented in this way may not be thought of as digital identity schemes by government or individuals, they nevertheless are based on a legal concept of identity. Most significantly, the individual's digital identity as registered under the scheme has specific transactional functions and standing. In this regard, the similarities between Australia and the United States are notable.<sup>10</sup>

In Australia, the foundations for a scheme of digital identity are being laid primarily through the national health care scheme which covers all registered Australians and eligible residents for medical care. The scheme has bipartisan support. In June 2010, for example, the Coalition supported the Labour 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.<sup>11</sup> This approach reflects similar developments in the United States.<sup>12</sup>

The move to digitalize government services in the United States has been underway for many years. In 2004, for example, electronic benefits and debit cards replaced paper food coupons. This system uses digital identity for transactions. Each recipient has an account in which benefits are electronically deposited each month. The recipient draws on the account in the checkout line of a grocery store, by sliding a plastic card through the same device used by other customers paying with commercial cards.<sup>13</sup> More recently, at a presentation on January 18, 2012,<sup>14</sup> the Chairman of the Federal Communications Commission spoke about the present Administration's objective to move all government services on-line<sup>15</sup> and the consequential objective to rollout broadband to most

---

Computers and Technology 8; Clare Sullivan, 'Identity or Privacy?' Special Issue: Identity, Privacy and New Technologies in (2008) 2(3) *International Journal of Intellectual Property Management* 289; Clare Sullivan, 'Who's Who – Conceptualising Identity' (2007) 21(3) *International Review of Law, Computers and Technology* 327. See also, Clare Sullivan, 'The United Kingdom Identity Cards Act 2006 – Proving Identity?' (2006) 3 *Macquarie Journal of Business Law* 259.

<sup>9</sup> The Indian scheme is almost identical to the United Kingdom scheme.

<sup>10</sup> Both countries have federal systems and a common law legal system. The ties between the two countries are historically closer than is generally known. Although Australia has a Westminster parliamentary system and is not a republic like the United States, the Australian Constitution is based on the United States Constitution, with the notable exception of the bill of rights. Some rights exist under the Constitution but most rights arise under common law or are enacted in state and federal legislation. Both Constitutions preserve states' rights, though it is generally fair to say that states' rights are more strongly defended in the United States than in Australia. Also, as observed by the Chief Justice of the High Court of Australia, Justice Murray Gleeson in the Boyer Lecture broadcast on Human Rights Day on 10 December 2000, "the Australian Constitution, as a plan of government for a federal union, is largely concerned with pragmatism rather than ideology".

<sup>11</sup> The Australian, "Coalition Eyes ID Card" <theaustralian.com.au> at August 24, 2010. In relation to the new Individual Healthcare Identifier ('IHI'), see the Office of the Privacy Commissioner <privacy.gov.au> at September 11, 2010. This is a significant development considering the checkered history of attempts to introduce a formal national identity scheme. The Australia card proposed in the 1980s led to national protests which resulted in the proposal being abandoned. In 2007, there was a further attempt to establish a national digital identity scheme, this time through the national health care system. The Australian health access card scheme did not meet with anywhere near the same level of popular resistance, probably because it was not presented as a national identity scheme and was given relatively little publicity. The scheme proceeded steadily through Parliament and was in Committee when there was a change of government. The introduction of the Access Card Bill in 2007 surprised many observers who assumed that it would not be introduced into Parliament until after the federal election in 2007. The Bill was introduced with comparatively little publicity, and after a very short period of public consultation. Its passage was not smooth and on 15 March 2007, it was delayed following a Senate Inquiry. Like the United Kingdom's Identity Cards Act 2006 (UK), on which it was clearly modeled, the Access Card Bill set out the framework for the new scheme and operational details including security and privacy aspects were to be covered in subsequent legislation. However, the Senate Inquiry recommended that the full legislative package be presented in one Bill, so that the entire scheme and all its consequences could be assessed. The government agreed, and the new Bill was to be introduced into Parliament in 2007, with a view to beginning the scheme in April 2008. However, the Federal election late in 2007 and the subsequent change of government led to the Access Card Bill being shelved, as the new government pursued different policy and funding objectives.

<sup>12</sup> Presentation by Julian Genachowski, Chairman of the Federal Communications Commission at "On the Record with TNR", The New Republic, at George Washington University, Washington DC January 18, 2012.

<sup>13</sup> It is important to note that the card is merely vehicle. It is the information which is important as is discussed in this paper.

<sup>14</sup> Ibid.

<sup>15</sup> See, USA.gov at <http://www.usa.gov/index.shtml> (last visited May 2, 2012).

Americans. This move necessarily requires authentication and verification of an individual's digital identity and as mentioned, all such schemes are founded on the premise of one person: one digital identity.

Significantly, the Australian government has now unequivocally stated that Australia is moving to "digital citizenship."<sup>16</sup> Considering the similarities in approach between Australia and the United States, the comments of the Australian Government in a recently released discussion paper<sup>17</sup> resonate with Australians and with Americans:

"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."

The paper also raises the issue of distribution of responsibility:

"... 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."<sup>18</sup>

Against this background, the next section of this paper examines the functions and legal nature of transaction identity. Transaction identity is the part of an individual's digital identity which is required for digital transactions. The implications for individuals, government and the private sector are considered.

### **Composition and Functions of Transaction Identity**

Transaction identity is a defined and limited set of information which determines an individual's identity for transactional purposes under the scheme. Transaction identity invariably comprises name, gender, date of birth, and a piece of 'identifying information.'<sup>19</sup>

A feature of all schemes which require digital identity for transactions is that the information needed to establish identity varies depending on the requirements of the transacting entity. In the United States typically, all that is required for routine transactions is full name, date of birth, gender and a signature. All or part of the social security number (SSN) may also be required, depending on the nature of the transaction.<sup>20</sup>

The information which comprises this transaction identity is defined and limited. It is largely information which is established at birth and it is relatively static in nature.<sup>21</sup>

In comparison, the other information which makes up digital identity is much more extensive and dynamic. The other information is augmented on an on-going basis. This other information tells a story about dealings and can be used to profile an individual. Even information which at first sight seems largely administrative adds to the profile. The other information is essentially personal information which is linked to an individual through transaction identity.

Transaction identity is the gateway to that other information. The system is designed so that transaction identity is the access point and transaction identity has a gate keeper role.

---

<sup>16</sup> Australian Government, "Connecting with Confidence: Optimising Australia's Digital Future" A Public Discussion Paper (2011).

<sup>17</sup> Ibid.

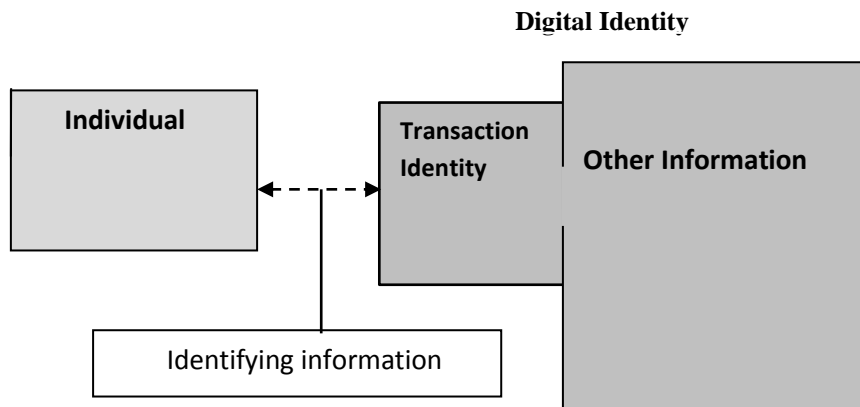
<sup>18</sup> Ibid.

<sup>19</sup> In some schemes such as those in Europe, identifying information includes biometrics, as well as a head and shoulders photograph. The usual biometrics are 10 fingerprints, two iris scans and a face scan.

<sup>20</sup> The social security number ("SSN") was originally used to identify United States citizens and residents for social security purposes but is now also used for taxation purposes. In practice, a social security number is required for many other purposes, such as opening a bank account or applying for a driving license. The SSN has therefore become a de facto national identification number in many states. However, this does not mean that it is necessarily part of transaction identity. The SSN is legally required for some matters. In many cases though, its provision is, or at least should be, voluntary.

<sup>21</sup> Other than in exceptional cases such as gender re-assignment, for example, the information which is most commonly subject to change is surname, mainly for women in the event of marriage.

The relationship between an individual and digital identity including transaction identity, can be depicted diagrammatically:



**Fig. 1.**

All digital identity schemes depend on two processes. These two processes are authentication of identity and verification of identity. Identity is authenticated at the time of registration. Identity is verified at the time of a transaction.<sup>22</sup> Although authentication and verification are often used interchangeably by commentators, this is typically the way these terms are defined for the purposes of the scheme. It was the approach used for the United Kingdom scheme, for example.

At registration, the information collected is used to authenticate identity in the sense that it is used to ‘to prove or serve to prove the authenticity<sup>23</sup> of the identity. Of the information recorded at that time, the identifying information such as signature or photograph<sup>24</sup> is used to the link an individual to the digital identity. This identifying information is regarded as being ‘identical with, or as associated inseparably with,’ that individual.<sup>25</sup> Under this type of scheme, there is an important distinction between identification and identity. Identification is just one part of the two processes used to establish identity.

Separately, the information which comprises transaction identity is diffuse and of limited use, even in identifying an individual. Unless it is especially unusual and unique, name alone for example, will not single out an individual from a large population. When the information is considered collectively, however, it takes on a different character which is greater than the sum of its parts. As a set, it becomes useful and valuable and its transactional functions give it specific legal character.

Transaction, identity is verified for transactional purposes when all the required transaction information presented, matches the information on record.<sup>26</sup> This matching is not with a human being. Transaction identity is verified by matching information. Through this matching process, transaction identity performs a number of vital, sequential functions.

---

<sup>23</sup> Definition of “authenticate” in the *Merriam Webster Dictionary*. The *Merriam Webster Dictionary* defines “authenticity” as “worthy of acceptance or belief as conforming to or based on fact;” “conforming to an original so as to produce essential features” and interestingly, “true to one’s own personality, spirit or character.” The latter meaning is significant in relation to the right to identity which is examined later in this paper.

<sup>24</sup> Photograph is distinguished from a face scan. A face scan is a biometric. In schemes which 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.

<sup>25</sup> “Identify” is defined in the *Merriam Webster Dictionary* as “to establish identity.”

<sup>26</sup> “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>.’

First, transaction identity identifies, by singling out one identity from all the identities registered under the scheme. The identifying information is used to identify the individual, though recall that not all the identifying information recorded under the scheme is generally required for a transaction.<sup>27</sup> The primary role of the identifying information is to link the digital identity to an individual person. Secondly, transaction identity verifies identity by determining whether there is a match between all the transaction identity information presented, with that on record.<sup>28</sup> These two steps enable the system to recognize and then transact.

Transaction identity does not just identify,<sup>29</sup> it enables the automated system to transact. Regardless of whether the transaction identity information is presented in person or remotely, if all the transaction identity information as presented, matches the information on record, then the system automatically authorizes dealings with that identity. The individual who is assumed to be represented by that identity is connected by the identifying information but a human being is not central to the transaction:

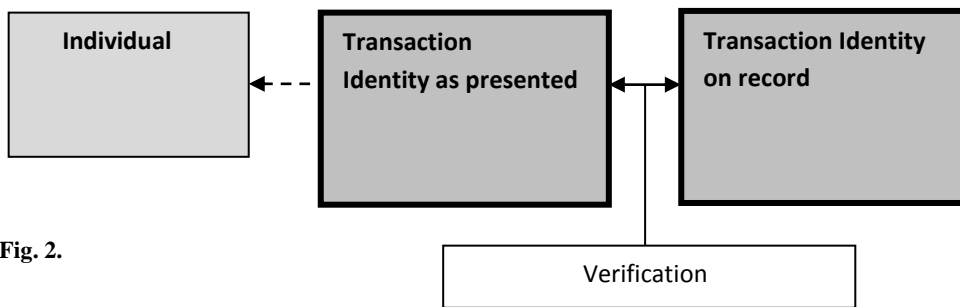


Fig. 2.

Of course, the assumption is that dealings are with the person who is presumed to be correctly represented by the registered transaction identity, which means that a transacting entity deals with that individual. The dealing would then be via the registered transaction identity but with the person:

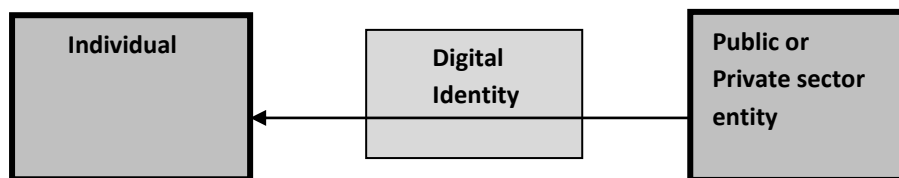


Fig. 3.

On this view, the information which constitutes transaction identity is just a credential, to be presented by an individual as part of the identification process, in much the same way identity papers are traditionally used. However, there are crucial differences.

<sup>27</sup> Especially for transactions conducted remotely, using telephone or the internet, for example.

<sup>28</sup> Such as name, date and place of birth as well as with signature, photograph and biometrics but bear in mind that not all transactions will use all the identifying information. Routine transactions may only require matching photo or signature. Many low value transactions such as those using the new Pay wave technology, do not require a signature or photo check.

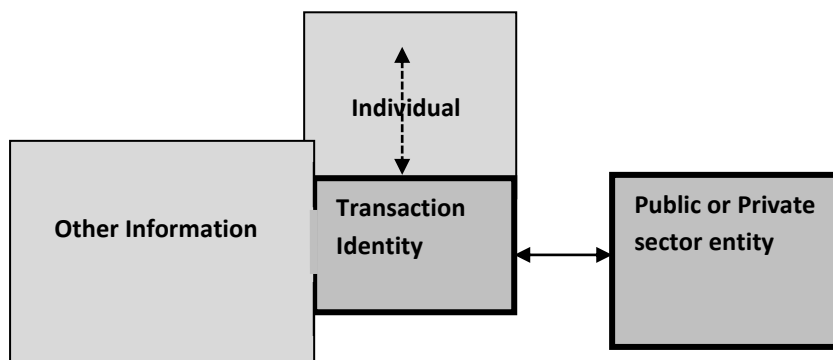
<sup>29</sup> Transaction identity extends beyond the identification requirements set out in the *Real ID Act* of 2005, Pub. L. No. 109-13, 119 Stat. 302, enacted May 11, 2005. The *Real ID Act* sets out requirements for State driver's licenses and ID cards in order for them to be accepted by the federal government for "official purposes", as defined by the Secretary of Homeland Security. The Secretary of Homeland Security currently defines "official purposes" as presentation of driver's licenses and identification cards for boarding commercially operated airline flights and entering federal buildings and nuclear power plants.

Traditionally, identity papers have been used to support claimed identity. Although the identification function of transaction identity may seem to replicate this traditional function, there is an important difference in the role played by human beings. Unlike traditional identity papers, the information which comprises transaction identity plays the critical role in the transaction, not an individual.<sup>30</sup> The system looks for a match between the information presented and the information on record.<sup>31</sup>

Transaction identity does not just identify. It has a much more important function. It *enables* the system to transact. This function gives it specific legal character and distinguishes it from identification procedures and requirements like those set out in the Real ID Act 2005.<sup>32</sup> While the Real ID Act could potentially set the foundation for a national identity card scheme in the United States,<sup>33</sup> at present Real ID does not include the functionality necessary to constitute transaction identity.<sup>34</sup>

Regardless of whether the transaction identity information is presented in person or remotely, if all the transaction identity information as presented, matches the information on record, then the system automatically authorizes dealings with that identity. Within these parameters the system ‘can act and will for itself’<sup>35</sup> to recognize the defined set of information which comprises transaction identity and then transact with that identity.

The individual who is assumed to be represented by that identity is connected by the identifying information but this link is relatively tenuous. A human being is not central to the transaction. The system and the transacting entity deals with the digital identity, via transaction identity, not with the person represented by that identity:



**Fig. 5.**

Although the assumption is that there is a reaching behind transaction identity to deal with a person, the system does not operate that way. If the transaction identity information presented at the time of a transaction, does not

<sup>30</sup>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.

<sup>31</sup> However, passports, particularly biometric passports, are now very close to transaction identity in functionality.

<sup>32</sup> These requirements include the provision of more documents, and information such as SSN, to obtain a State driver’s license or non-driver ID card, and specific information and security requirements for the license or card itself. The requirements are necessary for the license or card to be accepted by the federal government for "official purposes", as defined by the Secretary of Homeland Security. The Secretary of Homeland Security has currently defined "official purposes" as presentation of driver's licenses and identification cards for boarding commercially operated airline flights and entering federal buildings and nuclear power plants.

<sup>33</sup> The *Real ID Act* requires that a driver’s license or identification card requires, at a minimum, full legal name, date of birth, gender, signature, a unique identifying number, principal residence address and front-facing photograph of the individual in a common, machine-readable format. Driver’s licenses and cards must have specific security features designed to prevent tampering, counterfeiting, or duplication.

<sup>34</sup> Real ID also remains controversial and uncertain. States have been slow to comply because of concerns about compliance costs and civil liberties. All 50 States either applied for extensions of the original May 11, 2008 compliance deadline or have received unsolicited extensions. Thirteen states have now met the new deadline of May 11, 2011. For the other states, that deadline has since been extended to January 15, 2013.

<sup>35</sup> David Derham, "Theories of Legal Personality" in Leicester C. Webb (ed) *Legal Personality and Political Pluralism* (1958) 1, 14.



exactly match the record, the system will not recognize the identity and it will not transact. The system will not deal with the individual linked to that transaction identity,<sup>36</sup> even if it is otherwise authentic.

Procedures for dealing with this situation or to deal with people who for a variety of reasons are not registered,<sup>37</sup> illustrate the crucial function of transaction identity. Any protocol designed to deal with a situation in which an individual's transaction identity is not recognized by the system, must authorize dealings with the individual, not with the digital identity.

The authorization to transact, which occurs when the presented transaction identity information matches that on record, raises the question as to the legal nature of transaction identity. Who, or what, is the legal person in the transaction? Is it the individual who is connected to the identity in the scheme register, primarily by the 'identifying information'? Or is it the individual who presents the transaction identity? Although it is intended that be the same person, it may not be.

There is also an intriguing third option that transaction identity itself is the legal person. This invests transaction identity with legal personality, and it is a view which sits comfortably with its transactional functions. Its implications which are discussed in the next section, illustrate the inherent vulnerabilities of a scheme which uses digital identity for transactions, and the consequences for individuals, transacting entities and for the overall integrity of the scheme.

### **Transaction Identity as the Legal Person**

In the law, the legal person is the entity which bears legal rights and duties and so possesses what is called legal personality. Who, or what, is a person in law, is the subject of vigorous international intellectual debate. Central to this debate is whether the legal person must "approximate a metaphysical person."<sup>38</sup>

The orthodox positive view is that legal personality arises from rights and duties, rather than from intrinsic humanity.<sup>39</sup> In the words of Alexander Nekam: "[E]verything... can be the subject- a potential carrier – of rights."<sup>40</sup> "[T]here is nothing in the notion of the subject of rights which in itself, would necessarily, connect it with human personality, or even with anything experimentally existing."<sup>41</sup> Once a legal right is in evidence, so is a (legal) person.<sup>42</sup> According to Derham, "[I]t follows of course, that any 'thing' which is treated by the appropriate legal system as capable of entering legal relationships 'is' a legal person, whether it can act and will for itself or must be represented by some designated human being."<sup>43</sup> In other words, a "thing" can be

---

<sup>36</sup> The authenticity of a registered identity is clearly presumed, primarily on the basis that biometrics are reliable identifiers, and on the overall integrity of the scheme. There is obviously a presumption that the initial registration process is sufficiently robust to ensure authenticity and that subsequent use of the transaction identity is by the individual to whom it is attributed in the register. However, the 'identifying information' including biometrics, is not infallible. For a discussion of this aspect in relation to the United Kingdom National Identity Scheme, see Clare Sullivan, "The United Kingdom Identity Cards Act 2006 – Proving Identity?," (2006) Vol 3 *Macquarie Journal of Business Law* 259.

<sup>37</sup> These procedures balance equity and security concerns, with the balance likely to tip in favor of security.

<sup>38</sup> Ngaire Naffine, "Who are Law's Persons? From Cheshire Cats to Responsible Subjects" (2003) 66 *Modern Law Review*, 346.

<sup>39</sup> In Nekam's words, "[T]he rights themselves are given not for human personality or will but for the interests which the law-maker wants to protect." It is the socially protected interests which in legal abstraction we call rights. Since any conceivable interest attributed to any conceivable entity may be regarded as socially important by some community, anything may become a subject of rights – anything existing or anything to which the lawmaking community attaches any existence at all; and human personality or will is by no means a preliminary condition to its formation.' Alexander Nekam, *The Personality Conception of the Legal Entity* (1938), 27.

<sup>40</sup> Ibid, 26. See also Derham, above n 35, 13-15.

<sup>41</sup> Ibid, 26 and 28. Nekam asserts that the proposition that every individual is a natural subject of rights by virtue of his/her inherent humanity is flawed. However, as Nekam asserts, a connection between a right and a human being is inevitable. Nekam distinguishes the subject of the right from its administrator. While it is inevitable that the administrator of the right be human, the subject of the right need not be human.

<sup>42</sup> Margaret Davies and Ngaire Naffine, "Are Persons Property? Legal Debates Debates About Property and Personality" (2001), 54.

<sup>43</sup> Derham, above n 35, 13-15. Derham asserts that 'the wrong questions have been asked in the process of resolving many problems concerning legal personality.' He suggests that the appropriate questions are:

"[I]s there personateness? (a) Do the rules of the legal system establish that this entity.....is to be recognized as an entity for the purposes of legal reasoning (is to have the capacity to enter legal relations)?"

transformed into a legal person through the legal endowment of rights and duties.<sup>44</sup>The corporation is an obvious example of a thing which has been imbued with legal personality in this way. <sup>45</sup>

Transaction identity is similarly abstract and artificial. While a human being is linked to the registered transaction identity, through the identifying information, the transactional functions of transaction identity are not dependent on inherent humanity or on a legally competent, rational human actor. <sup>46</sup> Transaction identity is not colored by “metaphysical notions of what it means to be a person.”<sup>47</sup> Although there is a notional connection with a human being, it is the information which plays the crucial role in the transaction, not the individual to whom it is presumed to relate.

Richard Tur’s description of legal personality as “an empty slot”<sup>48</sup> that can be endowed with legal capacity is apt. Recall that verification of identity for a transaction involves two steps. Analogy can be drawn with a key being used to open a door. First, the transaction identity information is presented to establish identity; <sup>49</sup> like inserting the key into a lock - or a slot, to use Tur’s metaphor. In the second step, the presented information is compared with that on record in the chip on the card and/or in the register, to see if it matches.

The slot remains empty and non-functional until the key is inserted. If the information matches, it is like the indentions on the key aligning with the indentations in the slot which enable the key to open the door. When the transaction identity information presented matches that on record, rights and duties such as those arising under contract for example, then endow the ‘empty slot’, the transaction identity, with legal personhood. <sup>50</sup>

On this view, legal relations are between the registered digital identity and the transacting public or private sector entity. Transactional rights and duties initially attach to transaction identity and then to the registered digital identity:

---

*What is the personality?* (b) If so, do the rules of the legal system establish just what kinds of legal relations this entity may enter, or more commonly, do those rules establish whether or not this entity may enter the legal relation claimed or denied on its behalf?

*Should there be personateness?* (c) If the rules of law in (a) above are silent or ambiguous, should this entity be recognized as an entity for the purposes of legal reasoning?

*What kind of personality should there be?* (d) If either the rules of law in (a) or (b) above are silent or ambiguous and if (c), being relevant, is answered in the affirmative, then should the entity be recognized as having a personality which includes the capacity claimed or denied on its behalf to enter the legal relation concerned ?”

<sup>44</sup> As F. H. Lawson explains “[A]ll that is necessary for the existence of the person is that the lawmaker..... should decide to treat it as the subject of rights or other legal relations” F.H.Lawson, “The Creative Use of Legal Concepts” (1957) 32 *New York University Law Review* 909, 915.

<sup>45</sup> The argument that transaction identity is imbued with legal personality is most clear in the context of a national identity scheme established under legislation.

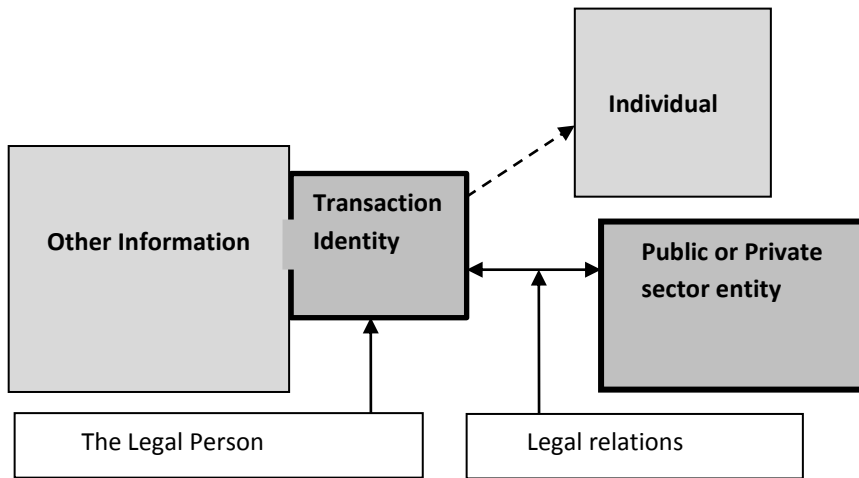
<sup>46</sup> A human administrator is required, however.

<sup>47</sup> Naffine, above n 38, 356.

<sup>48</sup> Richard Tur, “The ‘Person’ in Law” in A. Peacocke and G. Gillett (eds), (1987) *Persons and Personality: A Contemporary Inquiry*,123, 121

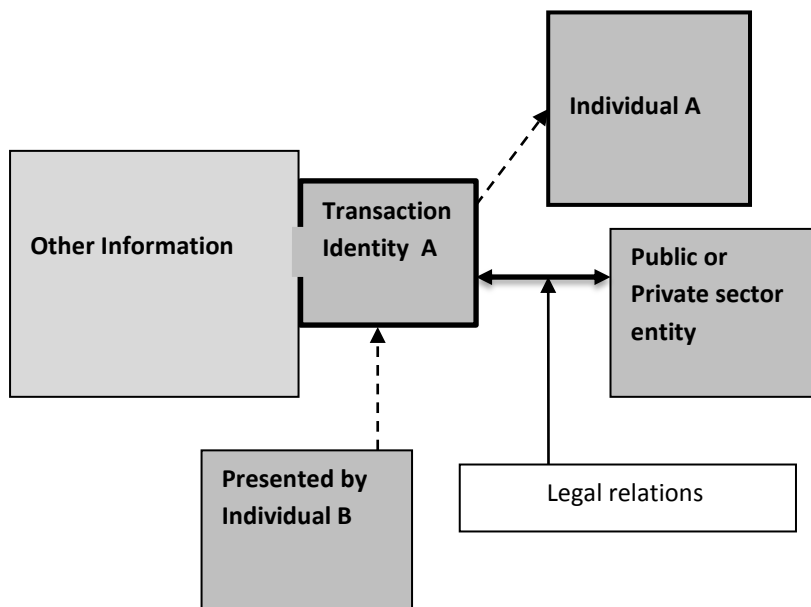
<sup>49</sup> Presentation may be by personal attendance at which time the information is provided by a person and/or a card is presented. The required information may also be provided by telephone or using the internet.

<sup>50</sup> This view of legal personality also accords with the enduring nature of identity. Identity, unlike privacy, does not necessarily cease on death though of course death affects the enforceability of rights and duties. Transaction identity usually includes date of death as well as date of birth.



**Fig.6.**

This raises the issue of responsibility. The basic principle is that for there to be a binding contract, an offer can only be accepted by the person to whom the offer is made. So what if individual B uses the transaction identity of another person A? The question then is whether the transacting entity intended to deal with A or with B:



**Fig.7.**

The answer to this question has depended on whether the transaction is face to face or by correspondence. If the transaction is face to face there is a presumption that the transacting entity intends to deal with the person who is physically present. Where the contract is in writing, only the person unequivocally identified in the written

contract is usually considered to be a party to the contract. But neither presumption fits well with contracts requiring digital identity.

If person B uses A's transaction identity, the person identified in writing in the contract is A. Face to face interaction does not usually translate well to transactions requiring digital identity but in terms of dealing, the public or private sector entity deals with transaction identity, not with the individual. Information and advice is provided to that registered identity. Invitations to treat and contracts are made with that identity but the public or private sector entity will, as a matter of practicality, look to the person linked to that identity under the scheme. In this example that individual is again A, although the transaction was orchestrated by B. This illustrates the legal and practical implications for an innocent individual.

If there is a possibility of error in authenticating identity at the time of registration, and/or in verifying identity at the time of a transaction (which of course there is, because no system is infallible), there are practical and legal issues. These issues impact on the integrity of the scheme and on all users, including transacting public and private sector entities, but the greatest impact is on the individual.

Transaction identity information can be miss-recorded or miss-read.<sup>51</sup> This can have consequences for an innocent individual which range from being unable to use the system using a legitimate, authentic digital identity, to an individual being the victim of identity theft and fraud. For example, system failure or fraud can result in the signature of B being recorded with the full name, gender and date of birth of another person A. In this scenario, the transacting entity will look to A because A's contact details including name are on record. This can present significant difficulty for A, who will then have to establish that he or she did not enter into this transaction. The implications can be serious. Imagine, for example, that A's identity information is used on-line to purchase a material used for bomb-making. That could make A the target of investigation for suspected terrorist activity. The consequences extend to reputation damage, bearing in mind that the other information which makes up digital identity records transactions on an on-going basis and can be used to profile an individual.

Not being able to transact under the system because an individual's otherwise authentic and legitimate digital identity is not recognized and functional also has significant impact which goes beyond frustration and inconvenience. In a world where digital identity will eventually be required for everything from employment applications and tax filing to welfare payments, being unable to use the system, even temporarily, can have serious consequences.

These aspects illustrate the need for fundamental individual rights to be recognized and protected. Considering the significance of transaction identity and the importance of ensuring it is accurate and functional, a range of rights and duties certainly arise in relation to it. Transacting entities using and relying on the scheme have rights and duties and the government has duties as administrator. The individual has associated duties regarding accuracy of information provided for registration and lawful use of the system, for example. The individual also has associated rights such as the right to register under the scheme.<sup>52</sup>

The most significant interest for the purposes of this discussion is the interest of the individual in the integrity and functionality of his or her digital identity. However, while the individual has a natural interest in protecting his or her digital identity, its accuracy and integrity also form the basis of the integrity and functionality of the scheme.

The argument presented in the next section is that the individual has rights in respect of his/her digital identity and specifically in relation to transaction identity, because of its specific functions under the scheme. The most significant individual rights are the right to privacy and the right to identity. Under the scheme the right to identity arguably takes specific form as the right to an accurate, functional digital identity. That right is examined as part of the broader right to identity, which is a recognized human right under international law. The nature and protection afforded by the right to identity is examined and is compared to the right to privacy.

---

<sup>51</sup> For a more detailed discussion of the fallibilities of identifying information, including biometrics, see Clare Sullivan, *Digital Identity* (2010) and the studies referred to in chapter 4.

<sup>52</sup> There is probably also a right not to register i.e. to opt out of the scheme.

## Digital Identity, the Right to Privacy and the Right to Identity

The right to identity as recognized under international law is conceptually very close to the right to privacy in that they both relate to individual autonomy. Nevertheless, they are separate and distinctly different rights. They are different in nature, they protect different interests, and they are infringed in different ways.

Both the right to identity and the right to privacy relate to autonomy. In the context of the scheme, that autonomy is an individual's right to self-determination in relation to information relating to him or her. However, the autonomy interest protected by the right to privacy is different from the autonomy protected by the right to identity.

Although the right to privacy can take different forms, in essence, privacy in the United States is infringed by the association of an individual with personal facts, contrary to the wishes of that individual.<sup>53</sup> By contrast, the right to identity is infringed by the untrue or false use of indicia of identity.<sup>54</sup> In the context of a scheme which requires digital identity for transactions, this indicia of identity is an individual's transaction identity.

Under the scheme, privacy is essentially about an individual's control over the collection, disclosure, and use of his or her personal information. The right to privacy clearly applies all the information which makes up an individual's digital identity.

The right to privacy can provide appropriate protection to the other information which makes up digital identity. Recall that this is the more detailed information which is updated on an on-going basis to reflect activity and changing circumstances. This is personal information which attracts protection under the right to privacy and under privacy legislation which regulates collection, use, disclosure and rights of access and correction. But the right to privacy does not clearly protect the set of information which constitutes an individual's transaction identity.

Unlike the other information which makes up digital identity, the information which comprises transaction identity is essentially public in nature. Information such as name, gender date of birth, signature, and /or photograph are in the public domain, in that this information is on public record or is either observable or freely disclosed. This presents difficulty for the right to privacy. While privacy protection can extend to information in the public domain, the information must be essentially private or intimate in nature to attract protection. It is unclear, and in fact doubtful,<sup>55</sup> that privacy protection applies to the information which comprises transaction identity because of its essentially public nature. Its public nature affects the protection that can be provided to the transaction identity information both individually and as a set.

Unlike the right to privacy, the right to identity fits well with the role of transaction identity under the scheme and the nature of the information which comprises it. This is because the right to identity is about autonomy in the sense of being recognized and regarded as a unique individual.<sup>56</sup> Given the nature of the scheme and that it is based on one person: one identity, the right to identity in this context must include the individual's right to a unique transaction identity and its exclusive use. Transaction identity is the means by which an individual is

---

<sup>53</sup> This is also true of privacy in Europe and Australia, although the right to privacy in the United States has developed along different lines. Now, however, there is noticeable convergence -the proposed principles in the Consumer Privacy Bill of Rights are based on the European data protection principles. The Privacy Principles in the Australian Privacy Act 1988 (Cth) are also based on the 1995/6 European model. In January 2012, however, the European Commission announced comprehensive reform of the EU's 1995/6 data protection rules to strengthen online privacy rights.

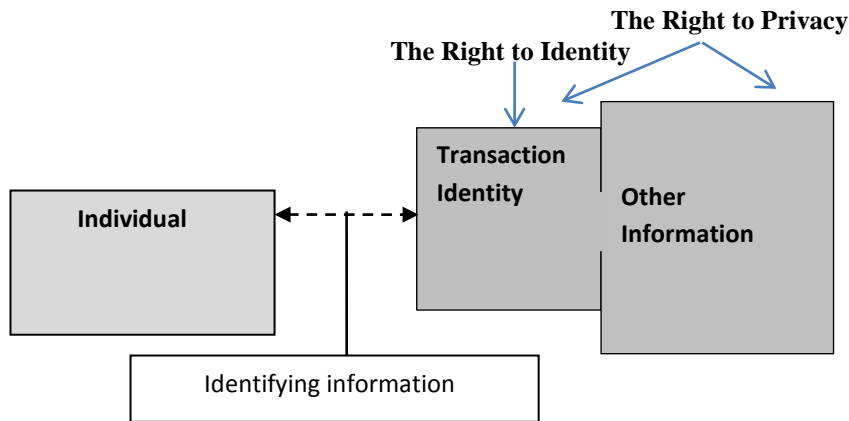
<sup>54</sup> J Neethling, J Potgeiter and P Visser, Neethling's *Law of Personality* (2005) ("Neethling"), 36. According to Neethling, "[i]dentity as an interest in personality, can be defined as a person's uniqueness or individuality which defines or individualises him as a particular person and thus distinguishes him from others. Identity is manifested in various indicia by which that particular person can be recognised; in other words, facets of his personality which are characteristic of or unique to him, such as his life history, his character, his name, his creditworthiness, his voice, his handwriting, his appearance (physical image), etcetera. A person has a definite interest in the uniqueness of his being and conduct being respected by outsiders. Therefore a person's identity is infringed if any of these indicia are used without authorization in ways which cannot be reconciled with his true image."

<sup>55</sup> For a more detailed discussion of this point, see Clare Sullivan "Digital Identity" 2010. See also Lynn M. LoPucki, "Did Privacy Cause Identity Theft?" (2002-2003) 54 *Hastings Law Journal* 1277 and "Human Identification Theory and the Identity Theft Problem" (2001 - 2002) 80 *Texas Law Review* 89.

<sup>56</sup> In an insightful passage, Neethling's *Law of Personality* distinguishes privacy from identity: "In contrast to identity, privacy is not infringed by the untrue or false use of the indicia of identity but through an acquaintance with (true) personal facts regarding the holder of the right contrary to his determination and will." See, J Neethling, J Potgeiter and P Visser, *Neethling's Law of Personality* (2005), 36.

recognized and regarded as unique. To maintain the integrity of the scheme and the transactions made under it, transaction identity must be protected from interference. The right to identity protects transaction identity from untrue or false use. Under the scheme, this right arises because of the key role played by transaction identity. The right to identity takes specific form as the right of an individual to an accurate, functional, unique transaction identity.<sup>57</sup>

The relationship of digital identity and the rights to privacy and identity can be depicted diagrammatically. The right to privacy forms an umbrella right that applies to all the digital identity information under the scheme, whereas the right to identity applies only to the set of information which constitutes an individual's transaction identity:



**Fig.9.**

The protection afforded to digital identity by the right to identity and the right to privacy differ because each right applies to a different autonomy interest. Most importantly, the right to identity and the right to privacy differ in the extent to which they can be subordinated to the public interest. This is important because the public interest can legitimately override individual privacy interests, especially in the interests of public safety and national security. As a consequence, the right to privacy also does not provide an appropriate level of protection to transaction identity.

Unlike the right to privacy, however, the right to identity cannot readily be subordinated to the public interest. In the context of the scheme, transaction identity is of such a fundamental nature that its interference or removal cannot be justified on public interest grounds. This is important considering the role and nature of transaction identity under the scheme, and the consequences for the individual, the government and the scheme if transaction identity is inaccurate, dysfunctional or is misused by another person.

The difference in the protection provided by the right to privacy in comparison to the right to identity is illustrated by the following example. Consider a person who has been convicted of a crime and is incarcerated. It is clear that in these circumstances, an individual's right to privacy does not prevent him or her being placed under surveillance in prison. Public safety considerations enable the prisoner to be kept under observation, and the loss of privacy is potentially total. However, even when incarcerated, a prisoner has a right to his or her identity and in a democracy that right to identity cannot legitimately be unilaterally removed, altered or made conditional on public interest grounds. The prisoner may be prevented from using his or her registered transaction identity for some transactions<sup>58</sup> but that is an entirely different matter from unilaterally removing or changing a person's identity or denying an individual the right to have a recognized identity. Unlike the right to privacy, the right to identity cannot be derogated in the public interest.<sup>59</sup> Infringement of an individual's right to

<sup>57</sup> The right to publicity may seem similar and in a sense it is but it protects a different interest in a fundamentally different way to the right to identity. The right to publicity also does not protect transaction identity, although it may protect a part of it, such as a photograph. The right to publicity protects an individual's image from use without permission or compensation, in much the same way as a trademark is protected.

<sup>58</sup> If the individual is prevented from using his or her transaction identity for all transactions, however, that would, in effect, be a denial of his or her right to identity under the scheme.

<sup>59</sup> It is doubtful whether there is any circumstance where unilateral interference with, or removal of, identity can be justified.

identity especially in the context of the scheme is unlikely to be justified because to do so gives the state power to disenfranchise an individual.

To maintain the integrity of the scheme, the registered identity of an individual must be protected from interference or disturbance. Unlike privacy, the right to identity is clearly capable of protecting transaction identity and provides more appropriate protection than the right to privacy at common law and under federal privacy legislation.

### **The Right to Identity in the United States under International law**

The Convention on the Rights of the Child expressly includes the right to identity.<sup>60</sup> The convention has been signed but not yet ratified by the United States.<sup>61</sup> Although the convention is not part of international law in the United States, signing is the first step in ratification. In signing the convention a state agrees to adhere to the principles in the convention and to honor its spirit.

The United States is one of only three member countries of the United Nations not to have ratified the convention, a fact which President Obama has described as “embarrassing.”<sup>62</sup> The Convention on the Rights of the Child is the most widely and rapidly ratified human rights treaty. Only the United States and Somalia, which has no functioning national government, have failed to ratify the treaty. Although the timetable for ratification is unknown, the United State should ratify the convention.<sup>63</sup> The argument presented in this paper is based on that occurrence.

The inclusion of the right to identity in Article 8 is significant because it shows that an express right to identity exists. The elements of identity specified in Article 8 also comprise some of the same information which constitutes digital identity, and the Article clearly distinguishes identity from privacy which is covered under Article 16.<sup>64</sup>

Article 8 specifically refers to the right to identity and to elements of an individual’s identity. Although ‘identity’ is not defined, Article 8(1) specifies that:

“States Parties undertake to respect the right of the child to preserve his or her *identity, including nationality, name and family relations* as recognised by law without unlawful interference.”<sup>65</sup> (emphasis added)

Article 8(2) further states that:

“Where a child is illegally deprived of *some or all of the elements of his/her identity*, States Parties shall provide appropriate assistance and protection, *with a view to speedily re-establishing his or her identity*” (emphases added).

---

<sup>60</sup> The convention was the first international treaty to cover a full range of civil, political, economic, social and cultural human rights in one document.

<sup>61</sup> In 2002, the United States ratified two optional protocols to the Convention on the Rights of the Child—one on the involvement of children in armed conflict (child soldiers) and another on the sale of children, child prostitution and child pornography.

<sup>62</sup> During his Presidential campaign in 2008, then Senator Obama reportedly said in relation to the Convention on the Rights of the Child: "It's important that the United States return to its position as a respected global leader and promoter of Human Rights. It's embarrassing to find ourselves in the company of Somalia, a lawless land. I will review this and other treaties and ensure that the United States resumes its global leadership in Human Rights." Walden University Presidential Youth Debate, October 2008.

<sup>63</sup> In 2002, the United States ratified two optional protocols to the Convention on the Rights of the Child—one on the involvement of children in armed conflict (child soldiers) and another on the sale of children, child prostitution and child pornography

<sup>64</sup> Art 16 *Convention on the Rights of the Child* states that, “No child shall be subjected to arbitrary and unlawful interference with his or her privacy, family, home or correspondence, or to unlawful attacks on his or her honour or reputation.” Art 18(2) states that, “The child has the right to the protection of the law against such interference or attacks.”

<sup>65</sup> Art 29(1)(c) which deals with the education of the child also mentions identity but it is identity in a different context and in a narrower sense — cultural identity

The concept of identity in Article 8(1) includes ‘name and family relations’ and ‘nationality’. This list is not exhaustive but the specific inclusion of these elements is significant considering the information which comprises transaction identity and that most of that information is to be registered at birth under Article 7(1).<sup>66</sup>

Article 8 was included in the Convention on the Rights of the Child as a result of a proposal by Argentina following a campaign by the Abuelas de Plaza de Mayo, the grandmothers of ‘The Disappeared’ in Argentina, for formal recognition of the right to identity.<sup>67</sup> The Abuelas alleged that in the 1970s the military junta systematically removed their children and grandchildren from their families and gave them a new legal identity as the children of other people. The Abuelas considered that Argentina’s adoption laws, at that time, concealed children’s true identities and enabled false identities to be created for them,<sup>68</sup> a concern which resonates with concerns about the integrity and protection of transaction identity.

Article 8(1) of the Convention on the Rights of the Child confirms the existence of a right to identity under international law. International law is, and should be, highly influential. It is a legitimate and important influence on the development of the common law, especially when international law declares the existence of a universal human right.<sup>69</sup>

The right to digital identity is arguably now part of the broader right to identity. In the context of the scheme, that right emerges on registration because at that time the prerequisites for registration are met, the required checks have been completed and the presumptions of accuracy and authenticity on which the scheme is founded, apply. At that time, the individual has the right to his or her registered identity and, specifically, to an, accurate, functional registered transaction identity and to its exclusive use. Unlike the right to privacy, this right of an individual to his or her registered identity cannot legitimately be readily curtailed or subordinated to the public interest.

The enduring nature of identity which is based on birth information and the rights of the individual in respect of that identity are evident when considered in the context of a witness protection program. If an individual is assigned a new identity under the program, the assignment must be with the individual’s consent and cooperation. Under a witness protection program, name and date and place of birth may be changed in the Births, Deaths and Marriages record, though witness protection legislation typically provides that the original details not be obliterated. Although the original record is screened from public view, it is retained and future restoration of the original identity is possible.<sup>70</sup>

In summary, the right to identity is about more than just control of personal information. It is the recognition that an individual has an inalienable ‘interest in the uniqueness of his being.’<sup>71</sup> The right to identity is a fundamental human right which arises at birth and which, unlike the right to privacy<sup>72</sup>, does not cease on death. The nature of that right and its origin are significant, particularly to the argument that the right to identity encompasses the right to transaction identity.<sup>73</sup>

In the context of a scheme which requires that digital identity be established for transactions, the right to identity is about an individual’s right to be recognised and to transact as a unique individual — in effect, to be

---

<sup>66</sup> Art 7(1) *Convention on the Rights of the Child* provides that, “The child shall be registered immediately after birth and shall have a right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents.”

<sup>67</sup> The original proposal was, “The child has the inalienable right to retain his true and genuine personal, legal and family identity. In the event that a child has been fraudulently deprived of some or all the elements of his identity, the State must give him special protection and assistance with a view to establishing his true and genuine identity as soon as possible. In particular, this obligation of the State includes restoring the child to his blood relations to be brought up.” See Sharon Detrick, “*The United Nations Convention on the Rights of the Child. A Guide to the “Travaux Préparatoires”*” (1992), 292.

<sup>68</sup> Their campaign resulted in Argentina recognising a constitutional right to identity and adopting an open adoption system. See Lisa Avery, “A Return to Life: The Right to Identity and the Right to Identify Argentina’s ‘Living Disappeared’” (2004) 27 *Harvard Women’s Law Journal* 235.

<sup>69</sup> The words of Justice Brennan of the High Court of Australia in *Mabo v Queensland (No 2)* [1992] HCA 23; (1992) 175 CLR 1, 42.

<sup>70</sup> See, for example, in Australia s 19 and s 11 Witness Protection Act 1994 (Cth).

<sup>71</sup> See J Neethling, J Potgeiter and P Visser, *Neethling’s Law of Personality* (2005), 36.

<sup>72</sup> The right to privacy is generally considered to be extinguished by death.

<sup>73</sup> However, protections under the convention only apply to children. In the United States, human rights of children and adults are protected by the Constitution and amendments, treaty, and through legislation enacted by Congress and state legislatures.



considered a unique entity under the scheme. Most importantly, given the nature of the scheme and that it is based on one person: one identity, the right to identity in this context must include the individual's right to a unique transaction identity and its exclusive use.

### **Recognition and Development of the Right to Transaction Identity in the United States**

The right to transaction identity in the context of an identity scheme is the right to be recognized and to transact under the scheme. Bearing in mind that that scheme applies to transactions with government and probably eventually with the private sector, the full import of this distinction is apparent if it is considered in the negative. In other words, if as a result of misuse or system failure, an individual's transaction identity is not recognized, the effect is to virtually render him or her non-person under the scheme.

Considering the functions and legal nature of transaction identity, and the consequences of misuse or system malfunction especially for an individual, a scheme of this type needs to be established within a regime that recognizes and protects individual rights including the right to identity as well as the right to privacy. There is scope for doing so in the United States.

The right to identity can be recognized and protected by legislation or recognized and protected as a common law right in much the same way as the courts have recognized the constitutional right to privacy in the United States. A full blown constitutional rights analysis is beyond the scope of this paper but the following is an outline of the type of argument that can be advanced to support this proposition.

The United States Constitution recognizes a number of inalienable human rights but not all rights are explicitly stated. The Ninth amendment specifically provides that "[T]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

Both the Ninth Amendment<sup>74</sup> and Fourteenth Amendment recognize that not all human rights have been enumerated.<sup>75</sup> As Justice Arthur Goldberg stated in a concurring opinion<sup>76</sup> in *Griswold v. Connecticut* <sup>77</sup>:

"...the Framers did not intend that the first eight amendments be construed to exhaust the basic and fundamental rights<sup>78</sup>....

...I do not mean to imply that the ... Ninth Amendment constitutes an independent source of rights protected from infringement by either the States or the Federal Government.<sup>79</sup>

...While the Ninth Amendment - and indeed the entire Bill of Rights - originally concerned restrictions upon federal power, the subsequently enacted Fourteenth Amendment prohibits the States as well from abridging fundamental personal liberties. And, the Ninth Amendment, in indicating that not all such liberties are specifically mentioned in the first eight amendments, is surely relevant in showing the existence of other fundamental personal rights, now protected from state, as well as federal, infringement. In sum, the Ninth Amendment simply lends strong support to the view that the "liberty" protected by the Fifth and Fourteenth Amendments from infringement by the Federal Government or the States is not restricted to rights specifically mentioned in the first eight amendments. Cf. *United Public Workers v. Mitchell*, 330 U.S. 75, 94-95."<sup>80</sup>

---

<sup>74</sup> The Ninth amendment states that "*The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.*"

<sup>75</sup> The rights stated in the Civil Rights Act of 1964 (Pub.L. 88-352, 78 Stat. 241(1964) and the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, § 2, 104 Stat. 328 (1991) are examples of human rights that were enumerated by Congress after the Constitution was drafted.

<sup>75</sup> *Griswold v. Connecticut* 381 US 479 (1965).

<sup>76</sup> With Justice Earl Warren and Justice William Brennan.

<sup>77</sup> 381 US 479.

<sup>78</sup> *Ibid*, 491.

<sup>79</sup> *Ibid*, 492.

<sup>80</sup> *Ibid*, 493.

The Ninth Amendment has been described as referring to "a universe of rights, possessed by the people — latent rights, still to be evoked and enacted into law....a reservoir of other, unenumerated rights that the people retain, which in time may be enacted into law."<sup>81</sup>

The right to identity is good example of such a right. The right to identity is undeniably a fundamental human right. As examined earlier in this paper, the right to identity is based on autonomy. It fits perfectly within "the "liberty" protected by the Fifth and Fourteenth Amendments from infringement by the Federal Government or the States."<sup>82</sup>

The other notable example is the right to privacy which is not expressly stated in the Constitution. In *Griswold v. Connecticut*<sup>83</sup> the Supreme Court ruled that the right to privacy is implied.<sup>84</sup> The case concerned a state law<sup>85</sup> but the reasoning in relation to individual autonomy and fundamental human rights generally resonate with the arguments presented in this paper in relation to the right to identity. Justice Goldberg, whom the Chief Justice and Justice Brennan concurred, found that the right to privacy to be "fundamental" because it "is of such a character that it cannot be denied without violating those fundamental principles of liberty and justice which lie at the base of our civil and political institutions."<sup>86</sup>

The right to privacy has since been developed by the courts to take into account changing lifestyle and technology as well as changing community standard and views<sup>87</sup> and privacy legislation has been enacted.<sup>88</sup> A similar argument can be advanced to support the recognition of the right to digital identity and specifically, the right to transaction identity. Recognition of the right of an individual to an, accurate, functional, unique registered transaction identity, and to its exclusive use, is fundamental to the individual's ability to be recognized and to transact under an identity scheme. In that context, the right to transaction identity is also of a character that it cannot be denied without violating fundamental principles of liberty and justice.<sup>89</sup>

## Conclusion

Digital identity is changing the way government interacts with its citizens and the nature of commercial transactions. Although the full import of this new era of digital citizenship is not yet known, it is clear that digital technology is no longer just as a means of collecting, storing and processing data and information. It is

---

<sup>81</sup> Remarks of Bernard Bailyn, Harvard University, at the Millennium Evening at the White House, 2000. This statement echoes ) the Sixth Circuit Court of Appeals in *Gibson v. Matthews*, 926 F.2d 532, 537 (6th Cir. 1991): "[T]he ninth amendment does not confer substantive rights in addition to those conferred by other portions of our governing law. The ninth amendment was added to the Bill of Rights to ensure that the maxim *expressio unius est exclusio alterius* would not be used at a later time to deny fundamental rights merely because they were not specifically enumerated in the Constitution."

<sup>82</sup> Justice Goldberg in *Griswold v. Connecticut* 381 US 479 (1965), 493.

<sup>83</sup> 381 U.S.479 (1965).

<sup>84</sup> Justice William O. Douglas wrote the majority opinion, finding that the right was in the "penumbras" and "emanations" of other constitutional protections. Justice Arthur Goldberg wrote a concurring opinion based on the Ninth Amendment. In a concurring rulings, Justice John Marshall Harlan II and Justice Byron White found that privacy is protected by the due process clause of the Fourteenth Amendment. Justice Hugo Black argued that the right to privacy is not to be found anywhere in the Constitution and criticized the interpretations of the Ninth and Fourteenth Amendments. Justice Potter Stewart called the Connecticut statute "an uncommonly silly law" but found that it was constitutional.

<sup>85</sup> The case concerned a Connecticut law that criminalized the encouragement or use of birth control. The Supreme Court ruled that the state's ban on the use of contraceptives violated the right to marital privacy.

<sup>86</sup> *Griswold v. Connecticut* 381 US 479 (1965). The paragraph states:"[I]n determining which rights are fundamental, judges are not left at large to decide cases in light of their personal and private notions. Rather, they must look to the "traditions and [collective] conscience of our people" to determine whether a principle is "so rooted [there] . . . as to be ranked as fundamental." *Snyder v. Massachusetts*, 291 U.S. 97, 105. The inquiry is whether a right involved "is of such a character that it cannot be denied without violating those `fundamental principles of liberty and justice which lie at the base of all our civil and political institutions' . . . ." *Powell v. Alabama*, 287 U.S. 45, 67. "Liberty" also "gains content from the emanations of . . . specific [constitutional] guarantees" and "from experience with the requirements of a free society." *Poe* [381 U.S. 479, 494] v. *Ullman*, 367 U.S. 497, 517 (dissenting opinion of Mr Justice Douglas),7."

<sup>87</sup> Over the next 10 years, the Court expanded the fundamental, substantive "right to privacy" beyond the marital bedroom, ruling that the state could not ban the use of contraceptives by anyone (*Eisenstadt v. Baird* 405 U.S. 438 (1972)) and that the state could not ban most abortions (*Roe v. Wade* 410 U.S. 113 (1973)). See also, *Bowers v. Hardwick*, 478 U.S. 186 (1986) and *Lawrence v. Texas*, 539 U.S. 558 (2003).

<sup>88</sup> Examples of other implied rights that have been recognized include the rights of former slaves through the abolition of slavery in 1865, the right of women to vote in 1920, the rights in the Civil Rights Act of 1964 (Pub.L. 88-352, 78 Stat. 241(1964) and the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, § 2, 104 Stat. 328 (1991).

<sup>89</sup> *Griswold v. Connecticut* 381 US 47 (1965).

embedded in processes fundamental to economic and social order. Digital identity and in particular, transaction identity, is the means by which an individual is recognized and interacts in this new environment.

As an emergent concept, digital identity and particularly transaction identity, is significant in its functions and its consequences. One person: one identity is a major change to the common law. The identity registered and used under the scheme will likely set the standard, so that its use covers not only dealings with government, but with private enterprise. What this means is that the identity used under the scheme becomes an individual's officially recognized identity for transactional purposes.

To date, legal scholarship and jurisprudence have looked to the law of privacy to protect personal information but as explained in this paper, transaction identity is more than just personal information. Transaction identity is a collection of designated information which is given legal status and effect by the scheme. When considered separately the information which comprises transaction identity is of little consequence. However, as a collective, that information has function as well as meaning and most significantly, it has legal character.

The focus on privacy has overshadowed the emergence of digital identity as a new legal concept and the consequential emergent identity rights. A right to identity is recognized under international law as a fundamental human right. In the context of an identity scheme that right now arguably encompasses a right to transaction identity.

The law in the United States is capable of recognizing a right to transaction identity just as it has recognized and developed the constitutional right to privacy in response to changing lifestyle and social mores. Considering the significance of digital identity in the context of the move to fully digitalize government services and the consequences for individuals, government and the private sector, this right to identity should be recognized in the United States.