III. Data Protection, Privacy and Identity: A Complex Triad

A. The Contours of Right to Privacy and Right to Data Protection

The concept of privacy is a multi-dimensional one, yet scholars across time and space have attempted to confine it to a single definition. Warren and Brandeis in their seminal essay enunciated that the right to privacy was based on a principle of "inviolate personality", thus laying the foundation for a concept of privacy, which we understand as control over one's own information.[42] Similarly, Westin defined privacy as:

> …claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.[43]

However, the many facets of privacy are better defined by breaking them down into categories, as done by Roger Clarke in his publications. Clarke identifies four categories of privacy viz., privacy of the person; of behaviour; of data; and of communication. Therefore, instead of equating privacy with data protection, Clarke's taxonomy allows different kinds of privacy to be protected differently. Accordingly, when this thesis discusses protecting personal data in the context of ensuring privacy, it does not in any way insinuate that all categories of privacy can be protected by way of protecting personal data.

The above discussion suggests a natural link between the right to privacy and the right to data protection. However, there is considerable academic discussion regarding the connection, or lack thereof, between the

---

42 Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, as cited in Judith DeCew, 'Privacy', The Stanford Encyclopedia of Philosophy, Spring 2015 <https://plato.stanford.edu/archives/spr2015/entries/privacy/> accessed 2 September 2017.

43 Alan F. Westin, 'Privacy and Freedom', Washington and Lee Law Review, Vol. 25 Issue 1 (1967) 7 <http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr> accessed 2 September 2017.

right to privacy and the right to data protection.[44] A strong case about the disconnect between data protection and privacy is made on the basis of the two distinct rights contained in Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union.[45] Article 7 of the Charter envisages the right to respect one's private and family life, home and communications, while Article 8 grants the right to the protection of personal data concerning oneself. However, in the absence of a specific right to data protection in Article 8 of the European Convention on Human Rights (ECHR), it materialises in conjunction with the jurisprudence of the European Court of Human Rights on the protection of privacy and private life.[46]

The author believes that although the Charter distinguishes the right to privacy and the right to data protection as two different fundamental rights, this is more in the nature of a formal distinction. It is doubtful whether the content of the two rights can be neatly isolated from each other.[47] This question may perhaps be answered by looking at the genesis of the right to data protection. Scholars in the field opine that the right to data protection has been characterized by strong links to the right to privacy.[48] Others like Van der Sloot are quick to point out the difference between the mandate for earlier Council of Europe instruments and the later engage-

---

44 Gloria Gonzales Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) Chapter 5; Raphael Gallert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 (5) Computer Law and Security Review 522; Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection Jurisprudence of the CJEU and ECtHR' (2013) 3(4) International Data Privacy Law 222; Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right' in Ronald Leenes et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017).

45 European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02. (Hereinafter *Charter*)

46 Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right' in Ronald Leenes et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017). See also ECtHR, *Amann v Switzerland* No. 27798/95, ECHR 2000-II, para. 65; *Rotaru v Romania* [GC] App no 28341/95, ECHR 2000-V, para. 43.

47 Raphael Gallert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29(5) Computer Law and Security Review 522, 524.

48 Gloria Gonzales Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) Chapter 5.

ment of the EU in the field of data protection.[49] Van der Sloot opines that while the main focus of the Council of Europe was to protect human rights on the European continent, the mandate to regulate data protection can be traced to market regulation and the facilitation of free flow of information.[50]

However, the line of argument delineating the right to privacy from the right to data protection does not work because today both these rights are enshrined in the Charter. Therefore, to say that the right to privacy is distinct from the right to data protection because the former is rooted in human rights while the latter is treated as an economic matter is a red herring to say the least. The CJEU in *Digital Rights Ireland* categorically highlighted the 'important role played by protection of personal data in light of fundamental right to respect for private life…'.[51] This approach taken by the CJEU is considered a human rights-based review.[52] Moreover, in the *Schrems* case, the CJEU retrospectively interpreted the DPD 1995 as implementing the right to data protection as guaranteed under Article 8 of the Charter.[53] The entire saga ties up neatly in light of Article 52.3 of the Charter – Article 52.3 provides that insofar as the Charter contains rights corresponding to those guaranteed by the ECHR, their meaning and scope shall be the same as that of the ECHR. What follows from this analysis is that the right to privacy as well as right to data protection under the Charter, and the right to privacy under the ECHR, need to be interpreted in a holistic manner.

Another attempt to sever the right to data protection from the right to privacy comes from the manner in which the GDPR is worded. Although unlike its predecessor, the GDPR does not contain any reference to the right to privacy, yet the author believes that this disconnect is merely

49 Van der Sloot, (n 46) 6; See also: Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), which envisages in Article 1 securing for every individual respect for 'right to privacy, with regard to automatic processing of personal data relating to him ("data protection")'.

50 Van der Sloot (n 46), 7.

51 CJEU, joined cases C-293/12 and C-594/12 (*Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others*), judgment of 8 April 2014, ECLI:EU:C:2014:238, para. 48.

52 Craig de Burca, 'EU Law: Text Cases and Materials' (6th edn, Oxford 2015) 401.

53 CJEU, case C-362/14 (*Maximillian Schrems v Data Protection Commissioner*), judgement of 6 October 2015, ECLI:EU:C:2015:650, para 78.

terminological. Regard being had to the jurisprudence of Europe's two highest courts (i.e., the ECtHR and the CJEU), the position which emerges is that data protection is an expression of the right to privacy.[54] The right to data protection is a nuanced right and builds on the premise that data processing is inadvertent. Accordingly, it follows that the GDPR contains detailed provisions regarding the obligations of the data controller and processor. These provisions on the right to data protection and what constitutes lawful processing are portrayed as a compromise between different legitimate interests. However, in the author's opinion, it does not serve the interests of either the data subject or the controller/processor to showcase their respective interests as being antagonistic to each other. The emphasis on how and when personal data can be legitimately processed is a corollary to the right to protect one's personal data. Regulatory initiatives to safeguard personal data have been grounded on privacy principles that can be used to identify problematic practices in the processing of personal data. Therefore, it is impossible to detach the right to data protection from the right to privacy.

With the relationship between right to privacy and right to data protection clarified, the next part seeks to establish the important connection between privacy and identity and the need for identity management in the framework of data protection. This will also lay the foundation for answering the research question by positing identity management as an effective tool for data protection.

B. Privacy and Identity: In the Shadow of Profiling

The notion of privacy has witnessed considerable shift in the digital age, due to the 'murky conceptual waters' between what is public and what is private.[55] This is especially so in the backdrop of profiling, where smart technologies are increasingly eroding privacy and the autonomy of individuals. Hilderbrandt defines profiling, albeit from a technological perspective, as:

---

54 Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection Jursiprudence of the CJEU and ECtHR' (2013) 3 (4) International Data Privacy Law 222.

55 Gary T Marx, 'Murky Conceptual Waters: The Public and The Private' (2001) 3 Ethics and Information Technology 157.

> …the process of 'discovering' patterns in data in databases that can be used to identify or represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent an individual subject or to identify as a member of a group (which can be an existing community or a 'discovered category').[56]

The GDPR contains a jargon-free definition of profiling which is easier to comprehend:

> 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[57]

Profiling has arisen as a new discipline combining data mining and statistics in order to profile the behaviour of users of an online service.[58] The issue of profiling has exacerbated in the context of IoT, where 'seemingly meaningless data generated by IoT sensors can be combined and analysed resulting in meaningful user profiles'.[59] Such indiscriminate profiling results in erosion of privacy and autonomy and is an assault on the very identity of an individual. Autonomic profiling is a precondition for 'smart' environments propelled by IoT.[60] Hilderbrandt explains autonomic profiling by way of comparing it to a futuristic human butler, where the nonhuman environment 'profiles' our needs and provides for their satisfaction.[61] Thus, autonomic profiling entails making decisions without the intervention of human consciousness. Although Hilderbrandt's analysis of profiling is done in the context of Ambient Intelligence (AmI), i.e., a concept developed to tap the idea of a 'smart' adaptive environment that re-

---

56 Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-disciplinary perspectives* (Springer 2008), 19.

57 GDPR art 4(1).

58 Jean-Marc Dinant, 'The Concepts of Identity and Identifiablity: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society?' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2009), 112.

59 Sarah Eskens, 'Profiling the European Consumer in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752010> accessed 10 September 2017.

60 Mireille Hilderbrandt, 'Profiling and AmI' in Kai Rennenberg, Denis Royer and André Deuker (eds), *The Future of Identity in the Information Society: Challenges and Opportunities* (Springer 2009), 287.

61 ibid 288.

quires little deliberate human intervention, her analysis resonates well with the goal being pursued by IoT.[62] Hilderbrandt postulates that autonomic profiling, which is a precondition for AmI, will significantly impact 'autonomous human action and the constitution of human identity'.[63] Furthermore, the means used to gather an individual's personal data, how the data is processed, and the lack of transparency surrounding its further use, stifles the personal autonomy and informational self-determination of the individual.[64] This is also an encroachment on the identity of an individual and involves data protection concerns.

Scholars have associated privacy with the notion of personhood and self-identity.[65] Likewise, the data protection ecosystem has incubated in the context of informational self-determination with guidance from the German Federal Supreme Court decision. The *Population Census* decision established informational self-determination as a constitutional right in Germany.[66] The right to informational self-determination has emerged as an important facet of the right of personality, which guarantees every individual the possibility to develop her own personality.[67] The German Federal Supreme Court found the legal basis for this right in a hybrid view of two separate provisions of the German constitution viz., right to dignity and right to general personal liberty.[68] Moreover, in linking privacy to autonomy, even the ECtHR has acknowledged that individual self-determi-

62 ibid 274.
63 ibid 290.
64 Neil M Richards and Jonathan H King, 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41 <www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/> accessed 10 September 2017.
65 N. Kanellopoulou, 'Legal Philosophical Dimensions of Privacy', EnCoRe Briefing Paper 2009 2.
66 Judgment of 15 December 1983, 1 BvR 209/83, BVerfGE 65 as cited in Gerrit Hornung and Christoph Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25 Computer Law and Security Review 84.
67 Gerrit Hornung and Christoph Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25 Computer Law and Security Review 84, 86.
68 Basic Law for the Federal Republic of Germany, art 1 para 1 and art 2 para 1 <www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0021> accessed 10 September 2017.

nation (or autonomy) is an important principle underlying its interpretation of Article 8 ECHR.[69]

There is literature supporting the idea that 'privacy protections are in essence protections of human dignity and personal autonomy'.[70] Given that the GDPR strives towards facilitating the data subject's ability to exercise control over her personal data (thereby embodying consent), it follows that personal autonomy is a key principle deeply entrenched in the fabric of GDPR. Therefore, the right to autonomy jurisprudence has significant importance in understanding the contours of data protection. As previously mentioned, right to data protection is interpreted by the CJEU by referring to the ECHR for guidance, and in light of Article 52.3 of the Charter by giving deference to the EctHR's case law. In *Pretty v UK*, the Strasbourg court expounded that the concept of 'private life' covers the physical and psychological integrity of a person.[71] In *Mikulic v Croatia*, the ECtHR opined that 'private life' embraces aspects of an individual's physical and social identity.[72] Broadening the concept of 'private life' further, the ECtHR in *Evans v UK* relied on previous case law and stated that private life encompasses the 'right to personal autonomy, personal development and the right to establish relationships with other human beings and the outside world'.[73] Personal autonomy emerges as a 'meta-value behind a number of individual fundamental rights'.[74] Another takeaway from the ECtHR's jurisprudence is the importance of safeguarding one's identity, as it is a crucial element of the right to autonomy.

Identity can be defined as a 'person's uniqueness or individuality which defines or individualizes him as a particular person and thus distinguishes him from others'.[75] An individual's identity manifests itself in various attributes, which make a particular person recognizable. These attributes are

69 Gallert and Gutwirth (n 47) 524.

70 Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge 2014), 12.

71 *Pretty v UK* [2002] ECHR 2346/02, para 61.

72 [2002] ECHR 53176/99 para 53.

73 [2006] ECHR 6339/05 para 57.

74 Manon Oostveen and Kristina Irion, 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?' in Mor Bakhoum et al (eds), *Personal Data in Competition, Consumer Protection and IP Law –Towards a Holistic Approach?* (Springer 2017).

75 Johann Neethling, 'Personality Rights: A Comparative Overview' (2005) 38 (2) Comparative and International Law Journal of Southern Africa 210 234.

unique to that particular person, like their life history, name, credit worthiness, voice, appearance, etc to mention a few.[76] A right to identity would thus mirror a person's inalienable 'interest in the uniqueness of his being'.[77] Information associated with an individual's identity is steadily becoming 'an essential enabler of today's digital society, as it is considered a key component in the interactions between end-users, service providers, and intermediaries.'[78]In that backdrop, the author believes that profiling leads to identity mutilation by intensive processing of personal data and de-individualises the individual. Yet, in the grander scheme of data protection outlined by the GDPR, identity is as marginalized as it was in the DPD – merely as a component of defining personal data.[79] Accordingly, in the absence of a distinct right to identity in the GDPR, safeguarding identity requires exercise of the available tools within the concept of lawful processing. The shortcomings of this approach are elaborated upon in the following discussion.

Autonomic profiling is specifically targeted in the GDPR by bringing it under the umbrella of automatic personal data processing.[80] Nevertheless, profiling is chastised in the circumstances where profiling produces 'legal effects' concerning the data subject or 'similarly significantly' affects the data subject.[81] The limitation of the right against being profiled only in so far as it produces 'legal effects', e.g., being rejected for a loan, being rejected for a job after an e-recruitment procedure, etc.) and grouping the myriad possibilities arising from profiling in a loosely worded manner, highlights the shortsightedness of this provision. The effectiveness of this provision is questionable in light of the complexity associated with profiling. For instance the nature of group profiling is that it represents a group and reveals the applicability of attributes to the individuals constituting

76 ibid.

77 Johann Neethling et al, *Neethling's Law of Personality* (Butterworths 1996) as cited in Norberto Andrade, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Simone Fischer-Hübner et al (eds), *Privacy and Identity Management for Life* (Springer 2010).

78 David Nuñez and Isaac Agudo, 'BlindIdM: A privacy-preserving approach for identity management as a service' (2014) 13 (2) International Journal of Information Security 199.

79 GDPR art 4(1) defines 'personal data' to mean any information relating to an identified or identifiable natural person.

80 GDPR recital 71.

81 GDPR art 22(1).

such a group.[82] This in turn means that the profile is not inferred solely from the personal data of the person so profiled, rather it makes use of large amount of data relating to many other people which may or may not be anonymised. The risk that emerges from this kind of profiling is more vicious than individual profiling because 'the process results in attributing certain characteristics to an individual derived from the probability that he or she belongs to a group and not from data communicated or collected about him or her.'[83] This strikes at the very identity of an individual and takes maintaining the sanctity of her identity beyond the realm of her personal autonomy.

Given that profiling threatens the identity of a data subject, it would serve the interests of the data subject if the GDPR acknowledged the complexity of profiling and addressed it by introducing a right to identity. Thus, automated data processing in the form of profiling could be confined more efficiently by having recourse to the right to identity. The right to identity may be introduced within the GDPR going a step further than the limited scope of an individual's right against automated profiling. Such an inclusion of the right to identity in the GDPR would provide the necessary mandate for putting in place an identity management solution to secure the protection of personal data. The following part buttresses the need for identity management and the role which blockchain technology can play in this regard.

C. Identity Management: The Blockchain Way Forward

In the information age, 'privacy paradox' lies at the core of the struggle for data protection. Privacy paradox is the unavoidable trade-off between the value of an individual's personal data and the value attached to their access to online services. The risk to an individual's identity stems from the indispensability of identity to certain transactions, for example, in determining the existence of necessary conditions for the transaction to oc-

82 Norberto Andrade, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Simone Fischer-Hübner et al (eds), *Privacy and Identity Management for Life* (Springer 2010) 102.

83 Yves Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?' in Serge Gutwirth, Yves Poullet and Paul de Hart (eds), *Data Protection in a Profiled World* (Springer 2010) 14.

cur, establishing a relationship for repeated transactions or tailoring delivery of products or services.[84] In order to enable such identity-requiring transactions, methods ought to be put in place to facilitate the asking and answering of identity queries.[85] Today digital identity systems have emerged as a reflex to the requirement of transactions in a digital world.[86] Risks to digital identity can come in the form of identity theft resulting from a privacy breach or dilution of identity arising from the inability to exercise control over the collection and processing of attributes. The need to part with personal data in order to establish one's identity, makes it imperative to have efficient tools to exercise control over what data is provided to the online service and how it is being used, i.e., collection and processing.

Ordinarily, control occurs at the start of a disclosure process; in this context privacy control is seen solely as a limitation on what personal data is made available to others.[87] However, in the era of Web 2.0 and IoT, it is seldom possible to exercise control at the initial stage of disclosing personal data because their architecture itself is premised on acquiring the personal data in order to give the user an enriched experience, or any experience for that matter. However, functionality does not warrant indiscriminate collection or processing of all sorts of personal data and there should be limits to the use and reuse of personal data. Therefore, in light of the preceding parts that establish a delicate balance between privacy, identity and data protection, it is imperative to envisage a scenario where identity management is a cornerstone to securing identity and protection of personal data. The previous part established that there are considerable risks involved in service-side storage and processing of personal information. When this is done without transparent and traceable relation to identities, it creates fundamental asymmetries in the relationship between the users and the online service providers. Therefore, user-centric identity management systems, which can restore this balance and confidence, are a

84 World Economic Forum, 'A Blueprint for Digital Identity' (August 2016) 32 <www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf> accessed 7 September 2017.

85 ibid.

86 ibid 36.

87 Edgar A. Whitley, 'Informational privacy, consent and the 'control' of personal data' (2009) 14 Information Security Technical Report 154, 155.

good response.[88]At the same time, it also calls for cautious pragmatism in choosing the tools used for identity management. The second chapter elucidates the basics of blockchain technology and the potential for using it to protect personal data. In this chapter, the author suggests that developing an identity management tool on the blockchain platform could be a more streamlined approach.

Identity Management platforms may be defined as systems that are 'used to support the management of digital identities or digital identity data'.[89] According to International Telecommunication Standardization Sector, identity management is used for:

– Assurance of identity information (e.g., identifiers, credentials, attributes);
– assurance of the identity of an entity (e.g., users, subscribers, groups, user devices, organisations, networks and service providers, network elements and objects, and virtual objects); and
– enabling business and security applications.[90]

For the purposes of this thesis, the focus will be on the utility of identity management to assure the identity of individuals using online services. In this context, identity management systems have tripartite participation from identity providers, relying parties and users.

Identity is a collection of attributes, which determine the transactions in which an individual can participate. The WEF Report categorises attributes as 'inherent, inherited and assigned'.[91] Table 1 illustrates what they mean in the context of an individual.

88 Simone Fischer-Hübner, C. Hoofnagle, I. Krontiris, K. Rannenberg, and M. Waidner (eds.), 'Online Privacy: Towards Information Self-Determination on the Internet', Dagstuhl Manifestos, Vol. 1 Issue 1 1–20 11.

89 Kai Rennenberg, Denis Royer and André Deuker (eds), *The Future of Identity in the Information Society: Challenges and Opportunities* (Springer 2009).

90 ITU-T, 'NGN Identity Management Framework', (2009) Recommendation Y.2720 1 < https://www.itu.int/rec/T-REC-Y.2720-200901-I> accessed 8 September 2017.

91 World Economic Forum (n 84) 41.

Table 1: Identity attributes in the context of an individual

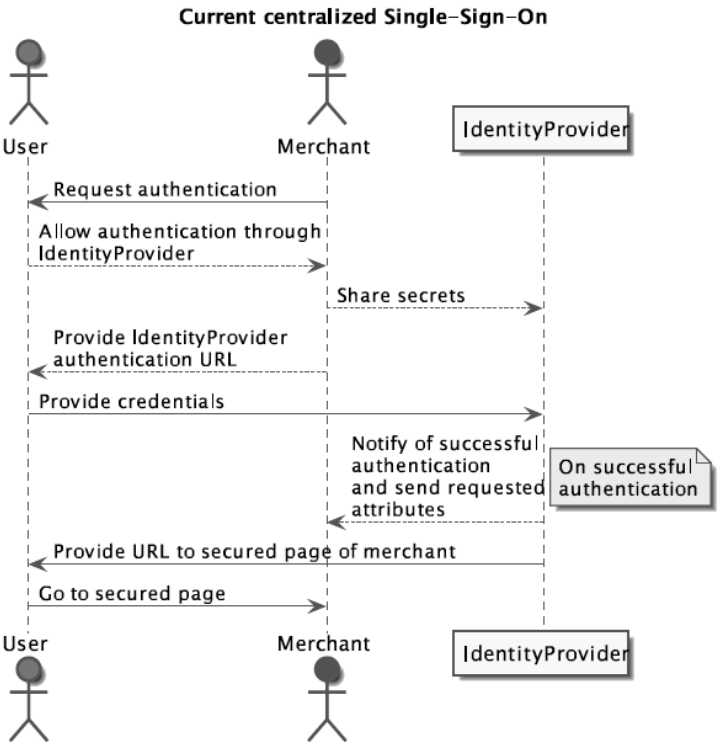
	For Individuals
Inherent Attributes Attributes that are intrinsic to an entity and are not defined by relationships to external entities.	Age Height Date of Birth Fingerprints
Accumulated Attributes Attributes that are gathered or developed over time. These attributes may change multiple times or evolve throughout an entity's life span.	Health records Preferences and behaviours (e.g., telephone metadata)
Assigned Attributes Attributes that are attached to the entity, but are not related to its intrinsic nature. These attributes can change and generally are reflective of relationships that the entity holds with other bodies.	National identifier number Telephone number Email address

Source: World Economic Forum (2016)

A transaction through digital channels relying on digital identity involves digital storage and exchange of attributes. An ideal digital identity management system would allow the sharing of their information (attributes) by exposing the minimum amount of information required for a given transaction, shielding their information from illicit access all along.[92] Organisations offering centralized identity management systems are able to track transactions enabling them to figure out the details of interactions using their system. Here is a pictorial representation to assist visualizing this problem:

92 World Economic Forum (n 84) 50.

Figure 1: Sequence Diagram of Centralised Single-Sign On



Source: Towards Self-Sovereign Identity Using Blockchain Technology (2016)[93]

Given the pitfalls of a centralised system, there is a strong case for shifting to an identity management system based on distributed identity. In a distributed identity system, multiple identity providers collect, store and transfer user attributes to multiple relying parties. The WEF Report iterates that distributed identity management systems are best suited to 'provide user convenience, control and privacy in an online environment'. This kind of identity management system can protect user privacy and enhance control by allowing users to choose which entities can hold their in-

93 Djuri Baars, 'Towards Self-Sovereign Identity Using Blockchain Technology', Master Thesis, University of Twente 2016 2 <http://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf> accessed 7 September 2017.

formation, removing a single point of failure from the system. [94] A distributed identity management system provides an entry point to blockchain technology, as the identity information is to be stored in a decentralized manner. [95]

The aim of this thesis is to propose a mechanism for minimizing the vulnerabilities faced by an individual in maintaining his digital identity within the ambit of the new personal data protection framework. The data protection framework shows some promise because it protects the attributes of identity in the form of 'personal data'. Using blockchain technology to build such a digital identity management platform would give it the required technological push.

Through a digital identity management platform, the data subject should be able to decide which attributes she is willing to disclose within the scope of permissions granted to a service provider. These permissions should govern the processing of data and can be revoked by the user of the digital identity management platform. Relying on the model proposed by Zyskin, Nathan and Pentland for personal data protection using blockchain may help in achieving this.[96] The fact that the access, storage and retrieval transactions are undertaken on the blockchain, it leaves an immutable trail of the manner in which access is provided conditional to permissions, which attributes are requested by a service provider and even how the personal data underlying these attributes is processed. This makes it easy for the data subject to exercise control over her attributes in the form of personal data. The blockchain approach is favoured over traditional identity management systems because the latter follows a centralized system characterized by single point of failure. Moreover, use of zero knowledge proof cryptography allows an identity owner to choose which identity information to reveal about herself and to prove claims about herself without revealing the underlying personal data.[97]

Currently, a few start-ups are leveraging the blockchain model to provide digital identity management platforms. Notable amongst these platforms are Sovrin and uPort.

Sovrin offers a permissioned blockchain that allows public access to identity owners but allows only trusted institutions to work as nodes on

94 World Economic Forum (n 84) 62.
95 World Economic Forum (n 84) 59.
96 Text to n 36.
97 Zyskin, Nathan and Pentland (n 36).

the network. It envisages an extra layer of verification of identity attribute asserted by an individual resulting in a decentralized identifier. Thereafter, claims made regarding one's identity are verified by accessing the relevant personal data, however, the blockchain can be tapped only for the decentralized identifier and the hashes/digital signatures of a claim, and not the personal data as such.[98]

uPort is a digital identity management service provided on the Ethereum blockchain network. uPort provides heightened levels of control to its users who can be fully in control of the identities created on this platform.[99] The MIT Human Dynamics lab as a part of their Core Identity Blockchain Project is also assessing the potential of uPort.[100]

Given that blockchain based digital identity management solutions are already offering their services, it becomes all the more important to analyse the compatibility of such a solution with the GDPR framework. Table 2 gives a brief overview of the possible interplay between the features of the proposed solution and the GDPR provisions.

Table 2: Mapping the GDPR provisions to blockchain powered DIM

Features of Blockchain powered DIM	**GDPR Provisions**
Decentralised transaction storage	Accountability
Replication of data over nodes	Data minimisation
Querying on a DIM platform	Control by Data Subject, Purpose and use limitation
Immutability	Right to be forgotten
Locking up of Data	Right to Data portability
Core features of blockchain	Data protection by design

98 Sovrin, 'Identity for all' <www.sovrin.org/> accessed 8 September 2017.

99 Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton and Michael Sena, 'Uport: A Platform for Self-Sovereign Identity' (21 February 2017) <https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf> accessed 8 September 2017.

100 Massachusetts Institute of Technology, 'Core Identity Blockchain Project' (2017) <https://law.mit.edu/blog/core-identity-blockchain-project> accessed 8 September 2017.