I. Introduction

We live in exciting times, where autonomous cars, smart homes and virtual currencies are not merely a creative scriptwriter's plot for an upcoming science fiction movie. These are real life manifestations of human effort, where erstwhile boundaries are being pushed to convert imagination to innovation. Much like any other form of progress, these developments are not happening in a vacuum. This engine of innovation is fuelled by data. According to a white paper by International Data Corporation, the *global datasphere*, i.e., the data created and copied annually, will reach a whopping 163 trillion gigabytes by 2025.[1] To put things into perspective, another study envisages that if the 44 trillion gigabytes were represented by the memory in a stack of iPad Air tablets (each 0.29" thick, having memory of 128 GB), there would be 6.6 such stacks from the Earth to the Moon.[2] While the simple, albeit over-simplified, assumption might be that much of this data would seemingly be impersonal, however in the context of modern data science Princeton University computer scientist Arvind Narayanan claims that the richness of data makes pinpointing people "algorithmically possible". This takes us to the conclusion that the more data there is out there, the less any of it can be said to be private.[3]

In light of the challenges posed by uneven harmonization and the fast pace of technological developments, the twin goals of data protection and free movement of data were falling through the cracks in the erstwhile Data Protection Directive 95/46/EC (DPD) regime. According to the Special Eurobarometer 2015, as many as 89% of surveyed Europeans acknowledged the importance of having the same rights over their personal infor-

---

1 David Reinsel, John Gantz and John Rydning, 'Data Age 2025: The Evolution of Data to Life-Critical' (April 2017) <www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf> accessed 27 August 2017.

2 Vernon Turner, 'The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things' (April 2014) <www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities-vernon-turner.htm> accessed 27 August 2017.

3 Patrick Tucker, 'Has Big Data made Anonymity Impossible?' MIT Technology Review - Business Report (7 May 2013) <www.technologyreview.com/s/514351/has-big-data-made-anonymity-impossible/?set=514341> accessed 27 August 2017.

mation, irrespective of the EU country in which it is collected and processed.[4] Moreover, the fact that 85% of the same people felt that they did not have complete control over the information they provided online pointed to the failure of DPD in inspiring trust.[5] It is in this context that the data protection ecosystem in Europe went through long-drawn reform eventually leading to the General Data Protection Regulation (GDPR).[6] The GDPR has replaced the DPD as of 25 May 2018, when it became directly applicable in each Member State of the EU amidst expectations of leading to a greater degree of harmonization in the realm of data protection across the EU countries. However, it is still to be seen how well the GDPR juxtaposes itself in the general landscape of data protection, most importantly how it integrates itself in a dynamic technological environment where the manner and rate at which data is processed is phenomenal.

Advances in the technology of storage and processing of personal data pose significant challenges for ensuring informational self-determination to data subjects. In line with Moore's law, sustained improvements in microprocessor technology have made the integration of digital features into everyday objects a reality that we today know as the Internet of Things (IoT).[7] This rapid progress is alarming because the highly connected nature of these 'things' makes profiling individuals a cakewalk.[8] It is a threat to their very identity and right to privacy. Red flags are being raised in data protection circles because data subjects are unable to have control over

4 TNS Opinion & Social, 'Data Protection' Special Eurobarometer 431 (June 2011) 10 <http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf> accessed 27 August 2017.

5 ibid 4.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> accessed 27 August 2017.

7 Moore's Law is a computing term which originated around 1970; the simplified version of this law states that processor speeds, or overall processing power for computers will double every two years. < http://www.mooreslaw.org/> accessed 27 August 2017.

8 Gartner Inc. had estimated that 4 billion connected things would be in use in consumer sector in 2016, set to rise to 13.5 billion by 2020.
Gartner Press Release, 'Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015' (Stamford, 10 November 2015) <www.gartner.com/newsroom/id/3165317> accessed 27 August 2017.

their own personal data. The threat to personal autonomy and identity of an individual has fuelled new approaches to rescue one's identity from drowning in the data deluge. With the reputation blockchain technology has garnered for itself in the short span of a decade, it posits itself as a possible solution to protecting personal data. A solution modelled on blockchain technology holds the promise of returning control to the data subject of her personal data and the ability to maintain the sanctity of her identity in the digital realm.

Thus, the research question that this thesis seeks to address is as under:

> Does the GDPR provide a conducive framework for a blockchain based digital identity management solution?

Answering this question calls for a techno-legal approach and entails a host of sub-questions. Before proposing a structure for the thesis, it is beneficial to list these sub-questions here:

- How is blockchain technology better placed to secure personal data protection?
- What is the relationship between right to privacy and right to data protection?
- Where does the concept of identity find itself in the discussion of privacy and data protection?
- Does the GDPR provide for safeguarding the data subject's identity?
- How is a digital identity management solution based on blockchain better than the existing means of identity management?
- Is the GDPR a technology neutral law?
- Does the GDPR, by itself, have the wherewithal to return control over personal data to the data subjects?
- Are all the principles of data protection in the GDPR to be accorded the same status?
- Is legitimate interest test an all-encompassing test?
- Is there an inherent contradiction between the goal of data protection by design and the other principles of the GDPR, especially in the context of blockchain technology?
- What are the suggested changes/interpretation to the GDPR?

At the outset, since the research question pertains to the compatibility of blockchain technology with the GDPR, it is imperative to introduce blockchain technology. The second chapter of this thesis attempts to put forth a simplified yet comprehensive description of all the essential concepts underlying blockchain technology. The chapter also discusses a

decentralized model for personal data protection built on blockchain. The third chapter deliberates on the nature of the relationship between right to privacy and right to data protection. It has been suggested that the only way to keep up with fast evolving data processing technologies is to ensure that the data subject has control over her personal data.[9] The notion of control emerges from the idea of enhancing autonomy of the data subject, germinating from the German doctrine of informational self-determination.[10] It appears that this right to informational self-determination integrates well with the aim of safeguarding one's identity and forms the basis for control of personal boundaries.[11] The discourse on privacy, data protection and identity leads to another essential concept from the research question –digital identity management. This is crucial in the era of the Web 2.0 and the Internet of Things (IoT), where profiling individuals is the backbone of their functionality and makes encroachments on the right to identity. Last part of the third chapter justifies the need for digital identity management in general and building this on a blockchain in particular. The fourth and most important chapter seeks to round up all the issues that may confront a blockchain-based solution of digital identity management in light of the GDPR. This chapter is crucial as it puts to test the claim that the GDPR is a technologically neutral legislation. It is also the right stage to question the applicability of new principles like right to be forgotten, right to data portability and data protection by design in the face of new technologies. Although this analysis comes in the nascency of GDPR, it presents a good opportunity to have an insight into the future of GDPR and its technological elasticity. The thesis concludes with a review of the obstacles and challenges expected to be faced by the GDPR on its way to realising the purpose of its promulgation, and how far blockchain technology is capable of assisting in this uphill task.

9 Scott R. Peppet, 'Unraveling privacy: The Personal Prospectus and the Threat of a Full-disclosure Future.' (2011) 105 Northwestern University Law Review 1153, 1183.

10 Volkszählungsurteil, BVerfGE Bd. 65, 1.

11 Irwin Altman, 'Privacy: A Conceptual Analysis' (1976) 8 Environment and Behavior 7-29. Altman conceives privacy as a "boundary control process"; the selective control over access to oneself.