THE UNIVERSITY *of* EDINBURGH

REVISITING THE LEGAL REGULATION OF DIGITAL IDENTITY IN THE LIGHT OF GLOBAL IMPLEMENTATION AND LOCAL DIFFERENCE

Rowena Edwardina Rodrigues

Doctor of Philosophy
University of Edinburgh
2011

Declaration

The work in this thesis is the candidate's own and has not been submitted for any other degree or professional qualification.

…….

Rowena Edwardina Rodrigues

Edinburgh

30 June 2011

Abstract

This thesis aims to address a vital gap that has emerged in the digital identity regulatory discourse: how can the legal regulation of digital identity mirror the global nature of digital identity and be compatible with national local difference?

Digital identity, or the digital representation of an individual, is a complex concept, which manifests in myriad forms (e.g. authenticators, claims, data or information, identifiers, presence, relationship representations and reputation) and natures. As such, it engages a gamut of legal domains ranging from criminal law, constitutional law, human rights law, law of identity schemes, contract law, intellectual property law, tort law and data protection law.

Digital identity is global and local in its nature, influence and effects. Yet, the digital identity regulatory discourse has primarily developed in and focussed on the digitally advanced West, leaving out countries like India which are developing strong digital presences, with their own digital identity perceptions and needs. This situation is adverse to the sustained future of digital identity. Thus, the contribution of this thesis lies in filling this gap and preparing the ground for a dialogue between different countries with different national agendas through building international and local awareness of how similarities and differences operate in respect of digital identity, its regulation and providing a modest solution to help preserve the global and local dimensions of digital identity and its regulation.

To this end, the thesis carried out comparative legal research on the legal regulation of digital identity using the UK and India as base jurisdictions. The original hypothesis was that that immense differences in the legal regulation of digital identity between the comparator countries would emerge. Yet, though differences were evident, considerable degrees of similarity also emerged, not just on the superficial level of mere identity of rules, but also in legal practice, in large part attributable to India's penchant for legal transplants.

While the transplantation of Western law did not result in a full-scale rejection of the transplanted laws in relation to digital identity in India, there are indications of anomalies caused by the imposition of Western cultural norms through law on an Indian society ill prepared for it. Thus there has resulted a tension between the local and the global, the indigenous and the externally imposed. The challenge is thus to resolve this, taking into account, on the one hand the need to maintain the global nature and relevance of digital identity and the other, the need to accommodate and be responsive to local differences.

The thesis proposes a tentative solution called the tri-elemental framework (TeF) which draws from the Indian philosophical and legal concept of *dharma* (and its elements of *Sad Achara, Vyavahāra and Prayaschitta*) and learns from the most universally relevant digital identity proposal, De Hert's right to identity. The solution provides one way in which the law regulating digital identity, whatever its nature, can be made sense of and acquire cultural meaning appropriate to local contexts.

Acknowledgements

I sincerely acknowledge the immense help, guidance and support of my supervisors, Professor Burkhard Schafer and Professor Lilian Edwards, from the initial days of my research right up to thesis completion.

I am also thankful to many and the following in particular for supporting my research in their professional and personal capacities: Professor Niamh Nic Shuibhne, Diane Whitehouse, Alistair Burnett, Trudy Burnett, Amanda Drollinger, Robin Gray, Julius Nayak, Dr Narayanan Unny, Dr Dinusha Mendis, SCRIPT and examiners Professor Paul De Hert and Dr Abbe Brown.

This thesis would not have been possible without the financial support of the University of Edinburgh in the form of the College of Humanities and Social Sciences Tuition Fee Scholarship and the Law Tercentenary ORS Award. For this, I am ever grateful.

Finally I thank my family, who have been there throughout, encouraging and bearing the brunt of it all, especially Romelo, Flavia, Jovito (without whom the journey would have been impossible) and Chloe Isla, my precious daughter.

Table of Contents

**All web links in thesis checked and accessible on 01.12.2010*

List of Abbreviations/Terms

AmI	Ambient Intelligence
CCTV	Closed Circuit Television
Ch/Chs	Chapter/chapters
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
FTC	Federal Trade Commission
GDP	Gross Domestic Product
ICANN	Internet Corporation for Assigned Names and Numbers
ICO	Information Commissioner's Office (UK)
ICT	Information and Communication Technologies
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IT	Information Technology
ITA 2000	Information Technology Act 2000
ITAA 2008	Information Technology Amendment Act 2008
ITU	International Telecommunications Union
MMORLGs	Massively-Multiplayer Online Real-Life/Rogue-Like (computer) Game
MMORPGs	Massively Multiplayer Online Role-Playing Game
n	footnote
NHS	National Health Service
Ofcom	Independent regulator and competition authority for the UK communications industries
OECD	Organisation for Economic Co-operation and Development
PC	Personal Computer
PRIME	Privacy and Identity Management for Europe
RFID	Radio Frequency Identification
s/ss	Section/sections
SC	Supreme Court (India)
SSO	Single Sign On
TRIPS	Trade-related Aspects of Intellectual Property Rights
UID	Unique Identity
UIDAI	Unique Identification Authority of India
UNCRC	United Nations
WAYF	Where Are You From
WoW	World of Warcraft
WSIS	World Summit on the Information Society

1. Introduction

"There are so many different viewpoints and that's why it's so difficult to create a rigorous model for digital identity."
-David Birch[1]

1.1. Overview

Digital identity[2] (defined as the digital representation of a digital identity subject[3] in tangible or intangible form, self-created, externally assigned or consequentially generated) is a pervasive, omnipresent and dynamic phenomenon of contemporary society with significant personal,[4] social, economic[5] and legal ramifications.[6]

There have been significant developments in the past decade (2000-2010) in relation to digital identity and identity management technologies, the law regulating such technologies and allied research in the digitally advanced West (digitally advanced Europe, the USA, Canada and Australia[7]). This is particularly evident in the growth of the identity management industry, legal regulation and the rise of digital identity initiatives like FIDIS,[8] the Identity Trail[9] and the Identity Commons.[10]

---

[1] David Birch, 'Issues and Concerns,' in Jane Adams and David Birch (eds), *The Digital Identity Reader 2007* (Mastodon Press, London 2007), 47
[2] For extensive coverage of the concept, see **Ch 2**.
[3] Digital identity, in the scope of this thesis, is largely restricted to that of human beings.
[4] An individual's life has become identity centric with individuals becoming, as Solove explains, creatures of "electronic collages" or "digital dossiers" that are used to identify and determine personhood. DJ Solove, *The Digital Person: Technology and Privacy in the Information Age* (NYUP, NY 2006), 2
[5] See H Abelson and L Lessig, 'Digital Identity in Cyberspace,' White Paper submitted for 6.805/Law of Cyberspace: Social Protocols (10 December 1998)
[6] See ITU, 'Internet Report 2006: Digital.life,' Chapter Four (Geneva, 2006) 93-120 <http://www.itu.int/osg/spu/publications/digitalife/docs/digital-life-web.pdf>; Solove (2006) **n4**; J Madelin and L Razzell, 'Towards an Identity Society,' White Paper, <http://www.identitysociety.org/files/identitysociety.pdf>; RA Bartle, *Designing Virtual Worlds* (Pearson Professional Education, NJ 2003), 159
[7] See R Clarke, 'Just Another Piece of Plastic for Your Wallet: The 'Australia Card' Scheme,' (1988) 18 (1) Computers & Society; GW Greenleaf and J Nolan, 'The Deceptive History of the Australia Card' (1986) 58 (4) Aust Qtly, 407-425; R Clarke, 'The Proposed Australian Implementation of the OECD Privacy Guidelines,' Working Paper (January 1987). See also C Sullivan, 'Digital Identity: An Emergent Legal Concept: An Analysis of the Role and Legal Nature of Digital Identity in a Transactional Context' (PhD Thesis, University of Adelaide 2009). Sullivan's thesis examines the law on ID Cards in the UK and Australia and shows that the two are similar in respect of their relationship with digital identity.
[8] The FIDIS Network of Excellence, a consortium of partners of industry and academia in Europe, was set up to explore the consequences of identity vis a vis privacy, security and trust. Its vision was to help Europe "develop a deeper understanding of how appropriate identification and ID management can progress the way to a fairer European information society." <http://www.fidis.net/>
[9] The Identity Trail, based in Canada, was a project involving North American and European researchers that explored three primary streams: the nature and value of anonymity, identity & authentication; the constitutional, legal and policy aspects and the development of technologies of identification, anonymisation and authentication. <http://www.idtrail.org>
[10] The US based Identity Commons is a community of working groups like the Identity Gang, the Internet Identity Workshop, Newbies for Newbies and Photogroup which aims "to support, facilitate, and promote the creation of an open identity layer for the Internet; one that maximizes control, convenience and privacy for the individual while encouraging the development of healthy, interoperable communities. <http://wiki.idcommons.net/Identity_Commons>

But digital identity is a phenomenon extending far beyond the digitally advanced West. Like identity, digital identity is fragmented, socially variable and despite its propensity to be a global technical construct,[11] is influenced by local conditionality, particularly in its legal regulation. Yet, there is very little in existing literature[12] on digital identity and its regulation beyond the digitally advanced West, in jurisdictions like India[13] which are emerging as significant markets for digital identity technologies like identity schemes,[14] the Internet,[15] mobiles [16] and RFID.[17]

At the wider international level, there is only one organisation with a noteworthy global thrust on digital identity: the ITU's Focus Group on Identity Management (FG IdM),[18] established in December 2006 (together with its allied initiatives the Joint Coordination Activity on Identity Management (JCA-IdM)[19] and the Global Standards Initiative for Identity Management (GSI-IdM)),[20] to "facilitate the development of a generic Identity Management framework, by fostering participation of all telecommunications and ICT experts on Identity Management."[21] Under the

[11] Digital identity technologies are universal in nature, unless specifically restricted. For example, a social networking profile in UK generally has the same technical features as a social networking profile in India. A biometric profile is universally relevant.
[12] As reviewed upto 2010.
[13] There are a few exceptions to this e.g. Costa Rica.
[14] India's UID project market itself is estimated at over Rupees 100 crore. See MB Chatterjee, 'Nine Submit Bids for UID Tender,' *The Hindu Business Line* (22 June 2010) <http://www.thehindubusinessline.com/2010/06/22/stories/2010062251760800.htm>; Brian Robertson, 'Indian ID Market Geared for Growth,' (2005) 17 (2) *Card Technology Today*, 11
[15] See Budde.Com, 'India - Internet Market,' Report, (05 July 2010) <http://www.budde.com.au/Research/India-Internet-Market.html>; IAMAI, 'Mobile Internet in India,' Report (December 2009) <http://www.iamai.in/Upload/Research/MobileInternetinIndia_39.pdf>; IAMAI & IMRB, 'Internet in India,' Report, (2007) <http://www.iamai.in/Upload/Research/I-Cube-2007-Summary-Report-final.pdf>
[16] India is one of the biggest and fastest growing mobile phone markets. IAMAI, 'Report on Mobile VAS in India,' (July 2010), <http://www.iamai.in/Upload/Research/Report_on_MVAS_(2010)_submittal_42.pdf>; 'The Next Billion Geeks: How the Mobile Internet Will Transform the BRICI Countries,' *The Economist* (Dadri, 2 September 2010) <http://www.economist.com/node/16944020?story_id=16944020&fsrc=rss>; R Blakely, 'When Prison is Just a Phone Call Away' *The Times* (India, 6 April 2009)
[17] RNCOS, 'Global RFID Market Analysis till 2010,' Strategic Report (August 2010)
[18] <http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html>
[19] <http://www.itu.int/ITU-T/jca/idm/>
[20] <http://www.itu.int/ITU-T/gsi/idm/>
[21] ITU-T, Focus Group on Identity Management, <http://www.itu.int/ITU-T/studygroups/com17/fgidm/>

auspices of the ITU, digital identity in jurisdictions like India has been explored either too broadly[22] or too technically.[23] This is a serious deficiency.

There are digital identity needs and regulatory interests beyond the Western digitally advanced world. Individuals in India, digital identity subjects like their Western counterparts, bring their life contexts to their experience and use of digital identity and are faced with the challenges of digital identity management and regulation, particularly in the light of the proliferation of digital identity technologies. But to date, there is no specific research exclusively exploring digital identity and its legal regulation in India and its consequent relation to and significance for global digital identity regulatory developments. [24] This situation is adverse to the regulatory future of digital identity, and the original contribution of this thesis lies in filling this gap.

This leads us to ask the central question of this thesis: "how can the legal regulation of digital identity mirror the global nature of digital identity and be compatible with national local difference?" The thesis aims to answer this question through a comparative study of the law regulating digital identity using the UK[25] and India[26] as base jurisdictions.[27] The UK is a prime example of a Western digitally advanced country and India is an example of a digitally advancing country. Both countries are

[22] See the manner of coverage of digital identity issues in India in the ITU primary document on digital identity. ITU Internet Report (2006) **n6**

[23] See R Ramamurthy, 'Data Theft and Identity Theft: A Review,' ITU Telecom World Geneva, 5-9 October 2009 <http://www.itu.int/tlc/WORLD2009/forum/entries/participant.148030.html>

[24] Existing research is patchwork and sectoral, focused on areas like outsourcing (mostly in relation to rights of data subjects of outsourced data), ID cards and not comprehensive enough to enable a holistic understanding of the complexity of legal and social issues involved.

[25] The UK comprises of England, Scotland, Wales and Northern Ireland. It is a constitutional monarchy with a parliamentary system of governance and a member of the EC since 1973. England and Wales follow the common law system, while Scotland has a mixed legal system (combination of common and civil law). Scots Law shares a number of statutory provisions with English law but its civil law is largely based on Scots common law rather than statute and has some Roman Dutch law elements. See HL MacQueen, 'Scots Law' in JM Smits (ed), *Elgar Encyclopaedia of Comparative Law* (Edward Elgar Publishing, Cheltenham 2006), 642-652; WDH Sellar, 'Scots Law: Mixed From the Very Beginning? A Tale of Two Receptions,' (2000) 4 EdinLR 3

[26] India is a federal republic of twenty eight states and seven union territories. Traditionally classified as an English Common Law System, it manifests the following distinctions: a written Constitution, separate personal law codes applicable to religious communities, no distinction between common law and equity and the tailoring of precedents to facts of the case.

[27] The thesis is novel in this respect. The only other comparative research into digital identity was carried out by Clare Sullivan in relation to transactional digital identity in the UK and Australia. See Sullivan (2009) **n7**

socio-culturally diverse[28] and ascribe different values to identity.[29] They are both very contrastive, yet digitally significant jurisdictions that struggle with issues of digital identity and its regulation.

1.2. Rationale and importance

Carrying out comparative legal research on the regulation of digital identity is a difficult task due to the high degree by which thinking about identity is culturally mediated.[30] Unlike technical aspects of law (e.g. corporate liability or investment fraud), identity touches upon the very manner one thinks about oneself, one's pre-theoretical and pre-legal, implicit and taken-for-granted assumptions of who one is and what it means to identify oneself as something or someone.

Indeed, on a meta-level one can query if asking these questions does not already bias the discussion towards a Western-centric approach where the existence of such a thing as the 'I' is much less controversial than in many Asian schools of thought. Contrast Descartes' self-confident '*Je pense, donc je suis'* that grounds knowledge of what he identified as the one base free of error, our notion of a thinking, indivisible self,[31] with the Buddhist notion of the empty, illusory and mis-identificatory self.[32]

---

[28] The UK is generally characterised as an individualist country and India as a collectivist country. See Geert Hofstede, *Culture's Consequences: International Differences in Work-related Values* (Sage, CA 1980); Geert Hofstede, *Cultures and Organizations, Software of the Mind: Intercultural Cooperation and its Importance for Survival* (Profile Books, London 1994),13-15; Charles Hampden-Turner and Fons Trompenaars, *Riding the Waves of Culture: Understanding Diversity in Global Business* (McGraw-Hill, NY 1997)

[29] See Nadia Tazi (ed), *Keywords Identity: For a Different Kind of Globalisation* (Other Press, NY 2004) (contrasting Europe and India); S Guha, 'The Politics of Identity and Enumeration in India c. 1600–1990,' (2003) 45 (1) Comp Studies in Society and History,148-167; Agehananda Bharati, 'The Self in Hindu Thought and Action,' in AJ Marsella, G DeVos and FL Hsu (eds), *Culture and Self: Asian and Western Perspectives* (Tavistock, London 1985), 185–230; B Cohn, "The Census, Social Structure and Objectification in South Asia" in B Cohn (ed), *An Anthropologist Among the Historians and Other Essays* (OUP, Delhi 1987), 224-254; Bidyut Chakrabarty (ed), *Communal Identity in India: its Construction and Articulation in the Twentieth Century* (OUP, New Delhi 2005)

[30] Clifford Geertz, *The Interpretation of Cultures* (Basic Books, NY 1973); A Swidler, 'Culture in Action: Symbols and Strategies,'(1986) 51 Am Soc Rev*,* 273-286; JE Cote & CG Levine, *Identity Formation, Agency and Culture: A Social Psychological Synthesis* (Lawrence Erlbaum Associates, NJ 2002)

[31] René Descartes *Discours de la Méthode* (1861)

[32] See *The Great Discourse on the Anattalakkhana Sutta,* (U Min Swe 1983); Paul Carus, *Gospel of Buddha* (Kessinger Publishing Co, Kila 2003); Martin Southwold, *Buddhism in Life* (Manchester University Press, Manchester 1983), 87

Nonetheless, we argue that comparative legal research that takes the cultural embeddedness of law seriously is a necessary, if difficult, pre-requisite for the sustained global regulation of digital lives.[33]

Two important international declarations accentuate the need for this thesis: the UN Millennium Declaration[34] and the WSIS Geneva Declaration of Principles for the Information Society. [35]

The UN Millennium Declaration recognises the need

> …through broad and sustained efforts to create a shared future, based upon our common humanity in all its diversity... These efforts must include policies and measures, at the global level, which correspond to the needs of developing countries and economies in transition and are formulated and implemented with their effective participation.[36]

This thesis, in explicitly highlighting and recognising the similarities and differences prevalent in the legal regulation of digital identity between countries, falls neatly within the framework of the Millennium Declaration and is a modest attempt to contribute to some of its goals.

The WSIS Geneva Declaration of Principles commits "to build a people-centred, inclusive and development-oriented Information Society."[37] It calls for raising awareness of the uneven distribution in "the benefits of the information technology revolution between the developed and developing countries and within societies,"[38] "digital solidarity,"[39] for stimulating respect for the "cultural identity, cultural and linguistic diversity, traditions and religions and fostering dialogue among cultures and civilizations."[40] For legal regulation to rise to this task, comparative legal

---

[33] G Wilson, 'Comparative Legal Scholarship' in Michael McConville, Wing Hong Chui (eds), *Research Methods for Law* (Edinburgh University Press, Edinburgh 2007), 87-103, 89
[34] UNGA Res 55/2 of 8 September 2000. UN Doc A/55/49 (2000)
[35] WSIS-03/GENEVA/DOC/4-E (2003), Geneva (12 December 2003) <http://www.itu.int/wsis/docs/geneva/official/dop.html>
[36] I.5
[37] Principle 1
[38] Principle 10
[39] Principle 17
[40] Principle 52

analysis that is cognisant of the wider socio-cultural factors that influence and shape our understanding of law, as provided in the thesis is required.

The need to revitalise the digital identity discourse through the scrutiny of alternative societies like India (rather than those dominating the discourse like the UK) also finds grounding in the works of Melisarris,[41] Menski[42] and Zittrain.[43] Melisarris and Menski both highlight the importance of studying how cultures can create alternative perceptions of the world and how this "framing" influences legal responses. This then translates for them into the need to allow different cultures to inform and advance the law in the global legal debate. Zittrain applies this theme directly to Internet governance, calling for the preservation of local understandings as key to successful Internet governance.[44]

This thesis subscribes deeply to these principles and goals and aims to fulfil their vision in preparing the ground for a dialogue between different countries with different national agendas through building international and local awareness of how similarities and differences operate in respect of digital identity and its regulation and providing a modest solution that will help preserve both the global and local dimensions of digital identity and its regulation.

1.3. Nature, method and scope

The research for this thesis originally set out with the hypothesis that immense differences in the legal regulation of digital identity between the comparator countries (UK and India) would emerge, and that the adoption of Western legal concepts thus far dominating the legal response in India would fail at the implementation level or create highly visible anomalies and efficiency loss.

---

[41] E Melissaris, 'The More The Merrier? A New Take On Legal Pluralism,'(2004) 13(1) Soc Leg Studies, 57-79, 76
[42] W Menski, *Comparative Law in a Global Context* (CUP, Cambridge 2006), 32
[43] Jonathan Zittrain, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law,' The Berkman Centre for Internet & Society, Harvard Law School Research Publication No. 2003-03, 5/2003 <http://cyber.law.harvard.edu/home/uploads/204/2003-03.pdf
[44] ibid

Since the cultural differences between the UK and India are arguably more deep-seated than those between European countries, and the issue of identity and its legal regulation more closely linked to non-legal cultural factors, one would expect a fortiori an even greater struggle for Indian society to live with regulations that express a value system and an approach to law in general, that is fundamentally alien. One therefore expected to find either that local solutions to identity regulation were emerging, or where this was not the case, imposed western-centric regulation was displaying systematic anomalies that needed addressing, with the indicators of such problems being: the non-application or inconsistent application of a law by the courts; failure to use available legal remedies by people who suffered harm due to ignorance or misunderstanding of the legal regime; failure in the uptake of technologies due to the fear of risks even where legal protection was available; systematic and widespread non-compliance with a law and an inability to adjust the legal regime flexibly to changing circumstances.[45] Indeed, a literature review reveals how this is the case in the inability of Asian countries to accommodate Western notions of rights.[46]

The analysis of law regulating digital identity in the thesis[47] reveals a slightly different picture, which is considerably more nuanced. While little in terms of indigenous legal solutions was found though differences were evident,[48] considerable degrees of similarity also emerged, not just on the superficial level of mere identity of rules, but also in legal practice, the "law in action."[49] Indian law is not perfect, but 'muddling through' by and large works. Noted comparatist Alan Watson's notion of

[45] This goes back to Legrand's concept of laws as "problem solving heuristics" which are impoverished when external transplants replace local legal problem solving methodologies. The recipient legal system in this case can follow blindly the new legal rules but lacks the deeper understanding to use them creatively to generate new legal concepts and solutions. See in particular, Pierre Legrand, *Against a European Civil Code* (1997) 60 MLR, 44- 63 (hereinafter (**1997a**). To use an analogy, it is easier for native speakers to develop language creatively by playing around with its rules than for a second language speaker who tends to adhere to them more rigidly.

[46] See eg, Russell Menyhart, 'Changing Identities and Changing Law: Possibilities for a Global Legal Culture,' (2003) 10 (2) Indiana J of Global Legal Studies, 157-199; RP Peerenboom, 'What's Wrong with Chinese Rights? Towards a Theory of Rights with Chinese Characteristics,'(1993) 29 (6) Harv Hum Rts J, 39-47; Sompong Sucharitkul, 'Thai Law and Buddhist Law,'(1998) 46 Am J Comp L, 69-72, 78; CM Cerna, 'Universality of Human Rights and Cultural Diversity: Implementation of Human Rights in Different Socio-Cultural Contexts,' (1994) 16 HRQ, 740-752

[47] **Chs 5, 6**

[48] **Chs 5, 6**

[49] For the distinction see eg, Esin Örücü, '*A Project: Comparative Law in Action*,' *in* E Örücü and D Nelkin (eds), *Comparative Law: A Handbook* (Hart, Oxford 2007), 435-499

legal transplants[50] accounts for much of this: India and the UK share a legal and political history and India adopted common law "as a block,"[51] just as Europe did with Roman law.[52]

Legal regulation (particularly in India) follows this trend by borrowing and adopting laws[53] in endeavouring to become compatible with international norms[54] or trade obligations[55] primarily those of the dominant countries, be it historically colonial powers like the UK or the US as leading force on the Internet.

However, Watson downplays the limitations of legal transplants, especially when enforced from above. Comparative legal research teaches us that top-down models of regulation are alien to the 'spirit of the people' (or the *Volksgeist* of Savigny) and problematic.'[56] When such models are adopted, legal enforcement and compliance suffer, efficiency is low and the legitimacy of the rules can be called into question -

[50] Defined by Watson as "the moving of a rule or system of law from one country to another or from one people to another." See Alan Watson, *Legal Transplants: An Approach to Comparative Law,* (Scottish Academic Press, Edinburgh 1974), 21. For more on legal transplants, see Alan Watson, *Comparative Law: Law, Reality and Society* (Vandeplas Publishing, FL 2008); Alan Watson, 'Comparative Law and Legal Change,'(1978) 37 CLJ, 313-336; Alan Watson, 'Legal Transplants and Law Reform' (1976) 92 LQR, 79-84

[51] Block reception, per Watson, is the main driving force behind legal change, and a common feature of legal development.

[52] Alan Watson, *The Making of the Civil Law* (HUP, MA 1981)

[53] This is particularly true of intellectual property and information technology law.

[54] This is evident in the case of the amendments to the IT Act 2000 by the IT Amendment Act 2008. Here, attempts have been made (rather carelessly, as it will later be shown) to transplant some elements of European data protection law like "sensitive personal data,"

[55] For instance as in the case of the TRIPS Agreement. India amended her intellectual property law in 1999, 2002, 2003 and 2005 to meet TRIPS obligations. Dr. KD Raju, 'WTO-TRIPS Obligations and Patent Amendments in India: A Critical Stocktaking' (2004) 9 JIPR, 242-259

[56] This term *Volksgeist* was coined by GW Friedrich Hegel. Savigny introduced this concept into law. Abraham Hayward (tr), *Friedrich Karl von Savigny, Of the Vocation of Our Age for Legislation and Jurisprudence* (Arno Press, NY 1975). Per this doctrine, law must come from custom and popular faith, then by judicial decisions and not by the arbitrary wills of lawmakers. This *Volksgeist* is differentiated from Montesquieu's *espirit de la nation* as an "active, creative but unconscious force that moulds a people's history and destiny." Michael Inwood, *A Hegel Dictionary* (Blackwell Publishers, Oxford 1992), 212. In India, Tilak recognised the need and importance of the *Volksgeist* in cautioning against the incautious adoption of law divorced from the historical and social context it operates in. JN Sharma, *The Political Thought of Lokmanya Bal Gangadhar Tilak* (Concept Publishing, New Delhi 2009), 97; VP Varma, *Modern Indian Political Thought* (Lakshmi Narain Agarwal, India 1971), 171

resulting in 'grey' jurisdictions that work their way around official state law.[57] This is typical of the Indian digital identity regulatory scenario.

Much of India's law regulating digital identity either has an imposed[58] or borrowed nature to it.[59] This often creates a mismatch between law on one hand and local needs, social value perceptions and practices on the other.[60] However, while the 'transplantation' of Western law did not result in an 'allergic reaction' in India, or a full-scale rejection of the transplant that the Legrandian approach predicts, there are indicators, if more nuanced ones that are indicative of anomalies caused by the imposition of Western cultural norms through law on Indian society ill prepared for it.[61]

In the case of digital identity, the tension between the local and the global, the indigenous and the externally imposed, is particularly poignant. This is illustrated by what we term the paradox of Internet regulation: On an abstract level, the Internet is simply a communication protocol. Communication works ideally when all communicating parties speak the same language. The introduction of dialects or idiolects makes communication difficult. Yet, simultaneously, communication requires the communication of different things or it becomes meaningless. Only in sharing differences can community really emerge. This in turn means that the efficient regulation of the Internet must be flexible and accommodating to local differences to give people an incentive to communicate, to make them feel secure and "at home." Any attempt at Internet regulation must balance the competing, equally meritorious and reasonable demands of the global and the local. The regulation of digital identity brings this tension to the fore. Digital identity technologies as global media ignore, to some extent, local peculiarities in the need to enable global access and communication.

---

[57] P Dalal, 'ICT Strategy of India Needs Rejuvenation,' (25 May 2007) <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN029840.pdf>; D Rodrik, 'World Too Complex for One-Size-Fits-All Models,' (2007) 44 *Post-Autistic Economics Review*, 73-74. See also **Ch 6**

[58] eg, the Indian Penal Code 1860, enacted during the British colonial period.

[59] A prime example is the Indian Constitution.

[60] **Ch 6**

[61] **Ch 6**

Here lies the problem. Not just for India but for all those countries facing a similar legal conundrum. The challenge lies in resolving this situation with a means that will take into account the need to maintain the global nature and relevance of digital identity as well as the need to accommodate and be responsive to local differences. Comparative law, where methodologically guided, can help find this balance. As indicated above, in comparative law, the tension between these two requirements is evident in the works of Watson[62] and Legrand.[63]

Watson who opines that "legal rules are equally at home in many places,"[64] emphasises the possibility and inevitability of legal transplants. Borrowing, per Watson, is common in law, vital to legal development and a means of perpetuating change in a legal system[65] to achieve legal harmonisation where this is politically and economically required.

Legrand denies the possibility of cross cultural legal fertilisation, given the differences in the underlying social fabric, philosophy and ways of life that are reflected in law.[66] He argues that "a crucial element of the ruleness of the rule - its meaning - does not survive the journey from one legal culture to another."[67] This is because law is embedded in the "legal mentalité" of a particular system.[68] This legal mentalité refers to underlying legal culture and epistemological assumptions of the system, the "way to see things."[69] For a Westerner, the sale of a cow may be a legal transaction identical to the sale of a pig, for a Hindu whose religious system sets cows apart from other animals; this equivalence is far from straightforward. Calling

[62] Watson (2008) **n50**; Watson (1978) **n50**; Watson (1976) **n50**; Watson (1974) **n50**
[63] Pierre Legrand, 'On the Singularity of Law,' (2006) 47 Harv Intl LJ 517-530; Pierre Legrand, 'The Same and the Different,' in P Legrand and R Munday (eds) *Comparative Legal Studies: Traditions and Transitions* (CUP, Cambridge 2003), 240–311; Pierre Legrand, 'What "Legal Transplants?' in David Nelken and Johannes Feest (eds) *Adapting Legal Cultures* (Hart Publishing, UK 2001), 55-68; Legrand (1997a) **n45;** Pierre Legrand, 'The Impossibility of "Legal Transplants,"'(1997) 4 Maastricht J Eur & Comp L, 111-124 (hereinafter **1997b**); Pierre Legrand, 'How to Compare Now' (1995) 16 LS 232
[64] Alan Watson, *Society and Legal Change* (Scottish Academic Press, Scotland 1977), 130
[65] Alan Watson, 'Legal Transplants and European Private Law,' (2000) 44 (2) EJCL <http://www.ejcl.org/ejcl/44/44-2.html>
[66] In similar vein, see Bernhard Grossfeld, *The Strength and Weakness of Comparative Law,* (Clarendon Press, Oxford 1990), 43
[67] Legrand (1997b) **n63,** 117
[68] Legrand (1995) **n63**
[69] Legrand (2006) **n63,** 522-25; Legrand (1997b) **n63**; Legrand (2001) **n63**, 55

both transactions a contract is simply glossing over the underlying conceptual differences, and differences in understanding, conceptualising and evaluating the situation.[70] Any legal conceptualisation of law opposed to life world experience is *un grande hazarde,*[71] and per Legrand, doomed to failure.[72]

The examination of legal regulation of digital identity in India in the thesis is proof that Legrand's belief is somewhat exaggerated. Many of India's laws are borrowed[73] and do seem to work more or less well despite her overwhelming non-western local culture.[74] At the same time, the thesis also illustrates how Watson's analysis is over optimistic, with serious problems becoming evident in the application and enforcement of the western approaches to law and digital identity regulation.[75] This thesis endeavours to develop a middle ground; a nuanced approach between these two positions. It recognises that to address India's needs in the legal regulation digital identity, western legal influences are unavoidable, but at the same time presents a framework whereby these influences can be assimilated in the light of local difference. The thesis proposes a tentative solution for the regulatory future of digital identity that is on the one hand, very abstract and capable of universal application if required and on the other hand, anchored in the *Volksgeist.*

---

[70] See also on this point Burkhard Schafer, Zenon Bankowski, 'Mistaken Identities: The Integrative Force of Private Law' in Mark Van Hoecke and Francois Ost (eds), *The Harmonisation of European Private Law* (Hart Publishing, Oxford 2000), 21-47

[71] As Montesquieu put it, "Les lois politiques et civiles de chaque nation . . . doivent être tellement propres au people pour lequel elles sont faites, que c'est un grand hazard si celles d'une nation peuvent convener à une autre." Montesquieu, *Esprit des Lois,* Book I, Chap. 3 (1758)

[72] Legrand (1997b) **n63**, 114; Also Tahirih V Lee, 'Risky Business: Courts, Culture and the Marketplace,' (1993) 47 U Miami L Rev, 1335-1414, 1335, 1338; Marcus Radetzki, 'From Communism to Capitalism in Laos: The Legal Dimension,' (1994) 34 (9) Asian Survey, 799-806, 799, 802

[73] The Indian Constitution is the best example of borrowed law in India. It borrowed from the UK (Parliamentary and cabinet form of governance, rule of law, concept of single citizenship, prerogative writs and bicameralism), the USA (fundamental rights, independent judiciary, judicial review, procedure for presidential impeachment, removal of SC judges etc), the Republic of Ireland (the Directive Principles of State Policy), Canada (its federal structure, advisory/review of the SC), Japan (procedures established by law), Australia (the Concurrent List and Freedom of Trade), the erstwhile USSR (the Preamble and fundamental duties) and Germany (emergency provisions).

[74] See **Ch 5**

[75] Substantiated in **Ch 6**.

This novel solution, called the tri-elemental framework (TeF), learns from De Hert's right to identity[76] and inherits from it a reliance on 'rights' as a key concept of legal regulation. This might be seen as Western centric in itself, but rights are identified here as the global "communication protocol of law," in the same way as 'http' is the communication protocol for the Internet.

De Hert's solution is more amenable to incorporate non-Western legal notions and concepts than other competing rights based approaches to identity regulation[77] which are more privacy centric, based on the individual autonomy and individual rights concepts which do not find social or cultural basis in jurisdictions like India.

Taking the right to identity as a starting point, the thesis develops the TeF, drawing from Indian philosophy and law, specifically the concept of *dharma*.[78] Thus, is provided one way in which the law regulating digital identity, whether of borrowed nature or not, can be made sense of and acquire cultural meaning appropriate to local contexts. It does in this sense not so much provide new legal mechanisms per se, but develops a conceptual framework that would make it easier for digital identity stakeholders to make sense of global legal concepts of digital regulation through the prism of their local lives and lived experiences. In the language of computing, the TeF acts as a compiler - a translation tool that translates one language into another, providing as a result the cultural embedding that legal transplants need to function at their best. On the more pragmatic level, it indicates teaching and communication avenues that can and should be used by the Indian authorities to explain and motivate regulation to their citizens and actors of the legal system.

---

[76] Paul De Hert, 'Right to Identity to Face the Internet of Things,' (2007) <http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf>

[77] **Ch 8**

[78] *Dharma* has both a legal and religious connotation. Religion is chosen as a source for conceptual inspiration because it provides a way of thinking about law more broadly than as a systems of state-based rules and institutions as Watson does, or a rational alternative to religious rites and ancestral customs. In the words of Davis, law, especially Hindu law, can itself be understood as a "theology of ordinary life." DR Davis, *The Spirit of Hindu Law* (CUP, Cambridge 2010). The solution proposed here is, therefore, not just valid for Hindus. Note that the author is a Catholic (part of the Indian religious minority).

Certain points must be clarified at this stage. The first relates to the position of the author vis a vis protective privacy standards. At various parts in the thesis, privacy is analysed from different perspectives (ie technical, legal). While this thesis presents privacy standards in relation to digital identity in a largely negative light (taking into account the cross-cultural dimensions, recognising that privacy is not contrary to popular belief a universal good), this is not to negate the importance of established standards in protecting digital identity,[79] only a call to be intuitive and responsive to local needs in relation to digital identity which manifests both global and local natures. The position adopted here is specifically not aimed to be reductionist.[80]

1.4. Structure

The thesis adopts the following structure: at the outset, it studies digital identity, local difference and digital identity management. This is followed by a meticulous examination of the law regulating digital identity. To bring out the complexities in the operation of this law, the application of the law is next analysed with the help of case studies. Then, key legal solutions proposed in respect of regulating digital identity are considered. This comparative analysis presents us with the main arguments of the thesis – of the inequality of global digital identity regulation and the need to find a middle path for the future. Finally, an attempt is made to present a way forward through a tri-elemental framework to guide the regulatory future of digital identity.

Chapter 2 focuses on digital identity. It examines the conceptualisation of digital identity, its multiple forms, presents its multivariate features and examines its relationship to the individual.

---

[79] Western (particularly European) technical and legal privacy standards are well established and generally work rather well to protect individuals from harms to their digital identity. There is scope in many respects for improvement but that debate is outwith the scope of this thesis.

[80] For instance, William L Prosser, 'Privacy,' (1960) 48 (3) California L Rev, 383-423; JJ Thomson, 'The Right to Privacy,' (1975) 4 Phil & Pub Affairs, 295-314; RA Posner, 'The Economics of Privacy,' The American Economic Review, 71 (2), Papers and Proceedings of the Ninety-Third Annual Meeting of the American Economic Association (May 1981), 405-409

Because digital identity, is connected to the individual (or the digital identity subject), it is affected and influenced local difference (a combination of digital developmental and social factors), which is examined in **Chapter 3**. The significance of this local difference has not been duly recognised or accounted for in the Western dominated digital identity discourse (regulatory or otherwise). This chapter aims to fill that gap by examining local difference in key digital identity contexts.

Identity management emerged as technical solution in the West to facilitate the creation, control and management of digital identities. **Chapter 4** charts the development and growth of the identity management in the private and public sector from centralised models of identity management to user centric models. Key issues highlighted in this chapter are the effectiveness of identity management as a technical regulator of digital identity. Also vitally examined is whether identity management takes into account the local peculiarities influencing digital identity.

Chapter 5 presents how the law regulates digital identity in the UK and India.[81] It presents and examines the different regulatory spaces occupied by digital identity and endeavours to elicit the nature of this regulation, given that while digital identity might have global natures, it is affected by local peculiarities. This is important because the legal literature in the West is largely concentrated upon issues of privacy and data protection in relation to digital identity and this chapter goes beyond this and makes a broader overview of the law.

Next, with the help of specially designed case studies, **Chapter 6** comparatively analyses the actual operation of the law in respect of key digital identity issues like privacy, sharing, reputation, anonymity, pseudonymity, access to Internet resources and control of personal data. This chapter aims to highlight the differences, if any that are evident in the actual operation of the law regulating digital identity, and what these differences mean for the global and national regulation of digital identity, particularly given local difference and the *Volksgeist.*

[81] While attempts have been made to comprehensively cover all law applicable to digital identities, it is noted that due to the evolving nature of digital identity there might be further scope for application of other areas of law to it, such as are not evident from the current state of the art.

Chapter 7 examines various legal solutions proposed in connection with digital identity: the constitutional right to virtual personality, the tort based right to identity, the right to database identity and De Hert's right to identity. This chapter critically analyses these solutions and their applicability in the light of how digital identity and its regulation is conditioned by local difference.

Finally, **Chapter 8** develops the TeF learning from De Hert's right to identity and inspired by *dharma*; accepting that while global influences are inevitable in digital identity regulation, there is a means, particularly for India to find local relevance in digital identity regulation. [82] Here, we come across another mainstay of the thesis: the advocacy for a move from a 'rights' based discussion of the legal regulation of digital identity to a more 'duty' based one that not only is in accord with the needs of countries like India but is also in accord with more recent European initiatives bringing back the focus on duties.

1.5. Contribution

This thesis contributes at many levels. First, through creating international awareness of both the similarities and the differences in respect of digital identity and its regulation, it will help boost international respect and cooperation[83] in regulating digital identity.

Second, it departs from the critiqued traditional comparative law approach of not recognising the role of socio-cultural context of law.[84] In conducting a deeper analysis of the socio-cultural contexts of the international differences evident in the legal regulation of digital identity, it goes beyond being a superficial analysis of the

[82] This corrects the deficiency in the international digital identity regulatory discourse of countries apart from the digitally advanced West not being able to make a significant and purposeful contribution.
[83] Roger Cotterrell, 'Seeking Similarity, Appreciating Difference: Comparative Law and Communities,' in Esin Örücü and A Harding (eds) *Comparative Law in the Twenty-First Century* (Kluwer, The Hague 2002), 35-54.
[84] Pierre Legrand, *Fragments on Law as Culture* (WEJ Tjeenk Willink, 1999) 6, 8

law regulating digital identity[85] and becomes more than a mere traditional legal comparative exercise.

Third, it will make local legislators, particularly in India, conscious of how borrowing and adopting laws to meet international obligations and new situations[86] without adapting them[87] to local conditionality might lead to their frustration.

Finally, in presenting a framework for the regulating digital identity capable of universal and simultaneous local application, it represents significant boost to the regulatory future of digital identity, particularly in terms of what countries like India, that have thus far operated on the periphery of the digital identity regulatory scenario can contribute to make its future their own too.

[85] One of the drawbacks of traditional comparative law identified is its propensity to skim surfaces. Lawrence Friedman 'Some Thoughts on Comparative Legal Cultures,' in DS Clark (ed), *Comparative and Private International Law: Essays in Honour of JH Merryman on his Seventieth Birthday* (Duncker and Humblot, Berlin1990), 49-57, 52; Legrand (1999) **n84,** 8

[86] Alan Watson, *Legal Origins and Legal Change* (CIP Group, London1990), 94; Lawrence Friedman, 'Some Comments on Cotterrell and Legal Transplants,' in David Nelken and Johannes Feest (eds), *Adapting Legal Cultures* (Hart Publishing, Oxford 2001), 93-99

[87] Efforts to adapt laws are limited. See Laurence Boisson de Chazournes and Vera Gowlland-Debbas (eds), *The International Legal System in Quest of Equity and Universality,* Liber Amicorum Georges Abi-Saab, (Martinus Nijhoff, Netherlands 2001), 415

2. Digital Identity: Definition and examination of forms and nature

> The search for identity is the ongoing struggle to arrest or slow down the flow, to solidify the fluid, to give form to the formless . . . Yet far from slowing the flow, let alone stopping it, identities are more like the spots of crust hardening time and again on the top of volcanic lava which melt and dissolve again before they have time to cool and set.
> *-Z Bauman*[88]

2.1. Introduction

In the 'Sound of Music' Maria sang, "Let's start at the very beginning, a very good place to start."[89] This chapter introduces digital identity, presents its forms, outlines it nature and the relationship with the individual (or the digital identity subject in the context of this thesis). This will help effectively negotiate the digital identity regulatory maze, which at the best of times can be highly complex and mystifying.

2.2. Identity

The English word 'identity' originated from the Latin root *idem* meaning 'the same.' It is defined as: a quality or condition of being the same, oneness, an instance of sameness, sameness of persons or entities in all circumstances, individuality, personality, personal or individual existence, or the 'self same thing.'[90] By definition, identity can thus be understood in different contexts and has different qualities like sameness, equality, recurrence, individuality, distinctiveness or existence.

Unlike the English definition, Indian languages do not have one comprehensive umbrella term that equates with the term "identity," though some languages like Hindi, Konkani and Marathi have adopted the Sanskrit root *asmita,* denoting identity, into their usage.[91] For example, Hindi, the official language of India, has various words denoting identity: *abhigyan* (recognition), *tatsmaka* (identity), *pehchan*

---

[88] Z Bauman, *Liquid Modernity* (Polity Press, Cambridge 2000), 82–83.
[89] Lyrics of Do-Re-Mi, in the Sound of Music by R Rodgers and O Hammerstein (1959)
[90] Oxford English Dictionary, <http://dictionary.oed.com/cgi/entry/50111220?query_type=word&queryword=+identity&first=1&max_to_show=10&sort_type=alpha&result_place=1&search_id=wr0i-HJbXtV-1860&hilite=50111220>
[91] See N Jayaram, 'Identity: A Semantic Exploration in India's Society and Culture,' in N Tazi (ed) *Keywords: Identity: For a Different Kind of Globalization* (Sage, Chennai 2004), 125-147,134

(identity, distinction or identification), *vyastitva* (identity), *shinakth* (identification) *samanta* (accordance or similarity), *sarupta (*identity or resemblance), *sarvsmik* and *tadatmay* (identity). In Konkani, there are a number of words in relation to identity e.g. *sar* (identity), *sama* (identical), *sama* (equal) *sarko* (similar) and *yekats* (one thing or identicality).[92] Marathi has the terms *parakh* (identification), *zasa* (similar), *manyata* (recognition or identification), *fark* (distinction, difference) and *ekadhyasarka* (alike).

But identity is not just a word; it is an ancient and contemporary fundamental human trait and the basis of human and individual existence and survival. By nature, it is complex and characteristic of many natures and elements like biography, biology, choices, genealogy, geography, interests, occupation, relationships, reputation, technology and transactions.[93] Identity is thus dependant and composite of many variables and factors. Though it may seem to have universality, it is highly globally variant[94] and plays to local cultural narratives, norms and conditions.

[92] See AFX Maffei, *English to Konkani Dictionary* (Asian Educational Services, 2007), 240
[93] A Cavoukian, 'Privacy in the Clouds, A White Paper on Privacy and Digital Identity: Implications for the Internet,' 28 May 2008 <http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf>
[94] Jean-Louis Nabki and Martine Ecolasse-Beilecki, 'Variants and Non-variants of Psychological Identity in Employed Females in Different Life Environments,' in Jose MariaPiero and others (eds), *Work and Organisational Psychology: European Contributions of the Nineties* (Taylor and Francis, Hove 1995), 47-60 (psychological global variance); MB Brewer and M Yuki, 'Culture and Social Identity,' in S Kitayama and D Cohen (eds), *Handbook of Cultural Psychology* (Guilford Publications, NY 2007), 307-322, 307

Identity has been studied in many disciplines: anthropology,[95] economics,[96] law,[97] political science,[98] psychology,[99] and sociology.[100] All of these demonstrate the complicated, contextual, dynamic, evolutionary, multi-dimensional and variant nature of identity, which is affected by cultural, economic, social, legal, political, psychological and spatial factors. As such, identity is a mercurial concept the law struggles to regulate.[101]

2.3. Digital identity: definition, examples and relationship with identity

Digital identity[102] is a conceptually complex term. It has been defined and interpreted in the different manners and contexts; as meaning one, some or a number of different things. This thesis defines digital identity as "the digital representation of an entity,

---

[95] A Cohen, *Self-Consciousness: An Alternative Anthropology of Identity* (Routledge, London 1994); For an interesting array of issues see M Sokefeld, 'Debating Self, Identity and Culture in Anthropology,' (1999) 40 (4) *Current Anthropology* 417-447.

[96] Ryan Patrick (ed), *Adam Smith: The Theory of Moral Sentiments* (Penguin Books, London 2010); GA Akerlof & RE Kranton, 'Economics and Identity,' (2000) 115 Quarterly Journal of Economics, 715; GA Akerlof & RE Kranton, 'Identity and the Economics of Organizations' (2005) 19 Journal of Economic Perspectives, 9; H Bodenhorn and CS Ruebeck, 'The Economics of Identity and the Endogeneity of Race,' NBER Working Paper Series 9962 (2003); R Bénabou and J Tirole, 'Identity, Dignity and Taboos: Beliefs as Assets,' IZA Discussion Paper Series (2007), 2583; P Chatterjee and S Sarangi, 'Social Identity and Group Lending,' Louisiana State University Departmental Working Papers, 2004-01 (examining the interaction between economics and identity in microfinance programs) (2004)

[97] Dan Danielsen and Karen Engle (eds), *After Identity: A Reader in Law and Culture* (Routledge, NY 1995); CL Cates & WV McIntosh, *Law and the Web of Society* (Georgetown University Press, Washington 2001), 129-152; J Marshall, *Personal Freedom Through Human Rights Law?Autonomy, Identity and Integrity under the European Convention on Human Rights* (Martinus Nijhoff, 2009)

[98] Amy Gutman, *Identity in Democracy* (Princeton University Press, 2003); J Caplan & J Torpey (eds), *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton University Press, 2001); Laura Dudley Jenkins, *Identity and Identification in India: Defining the Disadvantaged* (Routledge, London 2002)

[99] William James, *Principles of Psychology: Vol I* (Henry Holt, New York 1890); S Freud, 'The Ego and the Id,' in J Strachey and ors (eds), *The Standard Edition of the Complete Psychological Works of Sigmund Freud (SE) Vol. XIX,(1923-1925)* (Hogart Press, London 1974); MR Leary and JP Tangney, (eds), *Handbook of Self and Identity* (Guilford Press, NY 2003); TR Tyler, RM Kramer and OP John, (eds), *The Psychology of the Social Self* (Lawrence Erlbaum Associates, NJ 1999); MA Hogg and J Cooper (eds), *The Sage Handbook of Social Psychology* (Sage, London 2003). See also journal *Self and Identity*, Psychology Press, London.

[100] E Goffman, *The Presentation of Self in Everyday Life* (Doubleday, NY 1959); H Tajfel, *Human Groups and Social Categories: Studies in Social Psychology* (CUP, Cambridge 1981). For an overview of identity in the social sciences, see Anthony Elliot, *Handbook of Identity Studies* (Taylor & Francis, London 2011)

[101] Questions have been raised about the law's suitability and capacity to regulate identity: Eniko Horvath, *Mandating Identity: Citizenship, Kinship Laws and Plural Nationality in the European Union* (Kluwer Law International, Zuidpoolsingel 2008), 206; Carl Stychin, *Law's Desire: Sexuality and the Limits Of Justice* (Routledge, London 1995)

[102] Used in the thesis in both singular and plural senses.

in tangible or intangible form, self-created, externally assigned or consequentially generated."[103]

Digital identity is an identity mediated or experienced through the involvement and use of computer technology or digital communications like digital media or the Internet. It comes in various shapes:[104] account names,[105] Artificial Intelligence,[106] biometric data,[107] blogger ids, chat room ids, cookies, credentials, digital certificates, CCTV images,[108] digital images, digital/electronic signatures, DNA profiles, domain names, email ids, [109] e-portfolios,[110] geotags,[111] globally unique identifiers (GUIDs),[112] identity cards or tokens, instant messaging (IM) handles, InfoCards,[113] digital information, IP addresses, mobile identity[114] (e.g. IMSI number), passwords,

[103] This definition is resilient in its expression of digital identity as a representation. It is precise and dynamic enough to cover the different forms, account for the complex nature of digital identity and flexible to be adapted to future forms of digital identity.
[104] This list is not comprehensive. Digital identity has many other forms and is a constantly evolving creature.
[105] A series of letters and digits which uniquely identifies an account on a computer or on a network e.g. Login ID, User ID, or User Name.
[106] See D Cole, 'Artificial Intelligence and Personal Identity,' (1991) 88 (3) Synthese, 399-417; WJ Rapaport, 'Computer Processes and Virtual Persons: Comments on Cole's "Artificial Intelligence and Personal Identity," Technical Report 90-13 (Buffalo Dept. of Computer Science, May 1990).
[107] Biometric identity can be sub-categorised into: physical biometric identity or what we are, (fingerprints, facial recognition, hand geometry, iris scan, retinal scan, vascular patterns, DNA, neural wave analysis) and behavioural biometric identity that rely on the manner we do things (voice recognition, signature, foot dynamics and keystroke behaviour). E Mordini, and S Massari, 'Body, Biometrics and Identity,' (2008) 22 (9) Bioethics, 488-498, 488, 495; David Lyon, 'Biometrics, Identification and Surveillance,'(2008) 22 (9) Bioethics, 499-508
[108] M Carroll-Mayer, B Fairweather and BC Stahl, 'CCTV Identity Management and Implications for Criminal Justice: Some Considerations,' (2008) 5 (1) Surveillance and Society, 33-50 <http://www.surveillance-and-society.org/articles5(1)/identity.pdf>
[109] Email id is the baseline digital identity. See Norton Online Living Report 2009, <http://www.nortononlineliving.com/documents/NOLR_Report_09.pdf>
[110] An e-portfolio is a compilation of items like Web based text, electronic files, images, multimedia, blog entries and hyperlinks. Mhairi McAlpine, 'E-portfolios and Digital Identity: Some Issues for Discussion,'(2005) 2(4), E-Learning and Digital Media, 378-387; G Roberts and ors, 'Reflective Learning, Future Thinking: Digital Repositories, E-portfolios, Informal Learning and Ubiquitous Computing,' White Paper (2005) <http://www.alt.ac.uk/docs/ALT_SURF_ILTA_white_paper_2005.pdf>
[111] Geotags are geographical identification metadata added to various media like photographs, video, websites, or RSS feeds. FP Miller, AF Vandome and J McBrewster, *Geotagging* (VDM Publishing House Ltd, Beau Bassin 2009)
[112] A special type of identifier used in software applications to provide a unique reference number.
[113] Digital identities that individuals can use online and as implemented in Windows CardSpace, DigitalMe or Higgins Identity Selector. See **Ch 4 (4.5.3.1)**
[114] Referring here to "a message or set of linked messages derived from mobile computing devices and constituting claims about mobility, location or other characteristics which are assumed to represent a data subject." Els Soenens, "Mobile Identity and Location Based Services" in WP11, D11.4: Workshop on Mobility and Identity 20 April 2006, <http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp11-del11.4.workshop_on_MIDM.pdf>

personal data, personal profiles, public key certificates, reputation, RFID,[115] role-playing game (RPG) identities,[116] smart cards,[117] virtual identities like avatars,[118] wi-fi network names[119] etc. Some of these are often classed as sub-sets of digital identity, parts of, or composite digital identity. They can each exist in isolation, conjunction with and interact and intermingle across digital and non-digital worlds.[120]

At this point, it is highly useful to understand the relationship between digital identity and identity in general. The relationship between identity and digital identity cannot be understood in a single correct sense. Identity and digital identity have both simple and complex relationships, given that they are both complex concepts. In the simple sense, identity may be said to encompass digital identity, as depicted below:

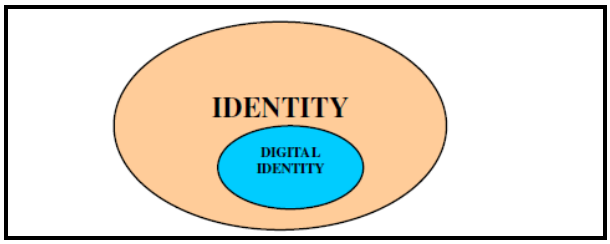

Fig 1: Identity encompasses digital identity

Identity is made up of more elements than just digital identity like body, values and beliefs, relations, social practices and habits, affiliations, interests, creations and

[115] RFID is a form of remote sensing technology that works through using radio waves to identify specific objects. RFID technologies are used to represent identity and facilitate identification, implemented in public transport cards, ID cards, passports, office identity tokens, loyalty cards, other access tokens, medical bracelets, tracking people, subcutaneous implants etc.
[116] As in Neverwinter Nights, Final Fantasy, WoW and Dungeons and Dragons. Hilde G Corneliussen, Jill Walker Rettberg (eds), *Digital Culture, Play, and Identity: A World of Warcraft® Reader* (MIT, USA 2008)
[117] Smart cards have strong identity content. They may be used for data storage, authentication, or identification. Examples of smart cards in the UK are the National ID card, London's Oyster card. In India, commonly used smart cards are Mumbai's BEST smart card, Gujarat's driving licence smart cards. More universal examples are payment cards e.g. MasterCard, Visa, American Express and Chase.
[118] See Ralph Schroeder (ed), *The Social Life of Avatars: Presence and Interaction in Shared Virtual Environments* (Springer, London 2001); Bruce Damer, *Avatars! Exploring and Building Virtual Worlds on the Internet* (Peachpit Press, 1998)
[119] D Boyd, M Chang and E Goodman, 'Representations of Digital Identity,' CSCW Workshop (6 November 2004) Chicago <http://people.ischool.berkeley.edu/~dmb/cscw2004-identity/IdentityWorkshopSubmission.pdf>
[120] D Greenwood, 'The Context for Identity Management Architectures and Trust Models,' Proceedings of the OECD Workshop on Digital Identity Management, Norway (2007)

choices, which may or may not influence or have bearing upon digital identity. The nature of the influence may vary. However, in some form or manner, it is inevitable that identity will influence digital identity. To substantiate, what one is or is not has a bearing on the digital identities one chooses to (or not to) express. [121]

Digital identity is a dynamic component of identity. It may form an essential part of it or a non-essential part. Digital identity, expressed in the above illustration as a single part, may itself comprise of different digital identities,[122] again all of which may have different relationships with identity that vary across time and space.

The complexity of the relationship between digital identity and identity thus becomes evident. What generates further difficulty is that digital identity is not an equal or stable part of identity, particularly in how it interacts with the other elements of identity.

Particularly, in the context of this thesis, it is extremely relevant to note international differences in this respect. While digital identity has become enmeshed with identity in Europe [123] in countries like India there are still fault lines evident in the relationship between digital identity and identity, which will become clearer as the thesis progresses. This is because the relationship between digital identity and

---

[121] These often seep into digital identity, as highlighted by Dahlberg. Ie, the content of online posts reveals information about the poster's affiliations, values, relationships, culture, gender and even geographical location. L Dahlberg, 'The Habermasian Public Sphere Encounters Cyber-Reality,' (2001) 8 (3) The Public, 83-96, 89

[122] As evidenced in: PJ Windley, *Digital Identity* (O'Reilly, USA 2005), 12; Jackie Marsh, *Popular Culture, New Media and Digital Literacy in Early Childhood* (Routledge, Falmer 2006), 126-143. The multiplicity of digital identities is also recognised throughout in DW Birch, *Digital Identity Management: Technological, Business and Social Implications* (Gower Publishing, England 2007); Ted Fair, Michael Nordfelt, Sandra Ring and Eric Cole, *Cyberspying: Tracking Your Family's (Sometimes) Secret Online Lives* (Syngress, MA 2005), 24, 296, 299; JRVacca, *Computer and Information Security Handbook* (Elsevier Science & Technology, MA 2009), 270, 271; Commission of the European Communities, Commission Staff Working Document, Accompanying Document to the Communication From the Commission to the European, Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, Future Networks and the Internet and Early Challenges Regarding the "Internet Of Things" Brussels, 29 September 2008, SEC (2008) 2516, para 3.2.4

[123] See Recommendation (a), European Parliament Recommendation of 26 March 2009 to the Council on Strengthening security and Fundamental Freedoms on the Internet. Text adopted on 26 March 2009. <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2009-0194>

identity in India functions differently as compared to the relationship between identity and digital identity in Europe.[124]

2.4. Forms of digital identity

An examination of the literature and the state of the art reveals the following forms of digital identity: authenticators, claims, data or information, identifiers, presence, relationship representations and reputation. These are now analysed respectively.

2.4.1. Authenticators

One of the most important forms of digital identity is an authenticator.[125] An authenticator is a token of authentication (or a credential) used to confirm or support identity.

The best example of an authenticator digital identity is biometric data.[126] Biometric data is defined as, "biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability."[127] It includes fingerprints, retinal patterns, facial structure, voice prints, hand geometry, vein patterns, deeply ingrained skill or other behavioural characteristics (like handwritten signature, keystrokes,[128] and movement and speech mannerisms).

---

[124] Further developed in **Ch 3**

[125] Windley (2005) **n122**, 50; John Mallery and ors, *Hardening Network Security* (McGraw-Hill Education, Europe 2004), 88; Economist Intelligence Unit, Digital Identity Authentication in E-commerce, *The Economist* (March 2007) <http://graphics.eiu.com/ebf/PDFs/IdenTrust_digital_authentication_Web_PDF_final.pdf>

[126] B Miller, 'Vital Signs of Identity,' (1994) 31 (2) IEEE Spectrum, 22 - 30

[127] Opinion 4/2007 on the Concept of Personal Data, Adopted on 20 June 2007, 01248/07/EN, WP 136

[128] R Joyce and G Gupta, 'User Authentication Based On Keystroke Latencies'; *Technical Report* 5, Department of Computer Science, James Cook University, Australia (1969); J Leggett, G Williams and D Umphress, 'Verification of User Identity via Keyboard Characteristics,' in JM Carey (ed), *Human Factors in Management Information Systems* (Ablex Publishing, NJ 1988) 29-42; D Umphress and G Williams, 'Identity Verification Through Keyboard Characteristics,' (1965) 2 (1) Int J Man-Machine Studies, 263-273

Another example of an authenticator is an electronic signature. Electronic signatures are, "data in an electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of information contained in the data message."[129] Electronic signatures validate and substantiate the identity of the signatory. They work like handwritten signatures and provide assurance and connectivity between a person and an object (generally a data message).

Other examples of authenticators are cookies, IDs and passwords, digital certificates and smart cards.

2.4.2. Claims

Digital identity may also take the form of claims. A claim is an assertion, a declaration or affirmation of a right to something. In law, a claim primarily signifies "the assertion of a right."[130] A claims based definition of digital identity is advanced in Cameron's 'Laws of Identity.'[131] Here, digital identity is defined as, "… a set of claims made by one digital subject about itself or another digital subject."[132] A claim is defined as the "an assertion of the truth of something, typically one which is disputed or in doubt,"[133] and a digital subject as "a person or thing represented or existing in the digital realm which is being described or dealt with,"[134] or in simple terms, the claimant.

The advantages of viewing digital identity as claims are elaborated thus by Cameron:[135]

1. It takes into account all identity systems and permits the conceptual unification of the "rational elements" of the patchwork.

---

[129] UNCITRAL Model Law on Electronic Signatures 2001, Art 2 (a)
[130] S Bone (ed), *Osborn's Concise Law Dictionary* (Sweet & Maxwell, 2001), 82
[131] K Cameron, 'The Laws of Identity,' Microsoft Corp (2005), 4 <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf> The Laws of Identity are a set of seven principles, developed by Microsoft's Kim Cameron and advanced through blogosphere discussions with different stakeholders to guide the development of Internet identity architectures and tools. The Laws are further discussed in **Ch 4.**
[132] Cameron (2005) **n131,** 4
[133] Cameron (2005) **n131,** 5
[134] Cameron (2005) **n131,** 5
[135] Cameron (2005) **n131**

2. It permits the definition of, "digital identity for a metasystem embracing *multiple implementations and ways of doing things.*[136]
3. It allows for the assertion of "things about another digital subject without using any unique identifier," by the subject.

However, Cameron acknowledges that the claims based definition does not bode well with the argument about the uniqueness of identities (i.e. in any given situation, identities are unique), which he refutes by advancing that the uniqueness of identities does not apply to all situations.[137] Cameron also opines that the definition "leaves the evaluation of the usefulness (or the truthfulness or the trustworthiness) of the claim to the relying party."[138] If the party evaluating the claim accepts it, then that decision simply is representative of a further claim in regards to the subject.[139]

The OECD also supports a claims based characterisation of digital identity.[140] It adopts the definition used by the Identity Gang:[141] "a digital representation of a set of claims made by one party about itself or another data subject."[142] Digital identity is also viewed as claims by the Liberty Alliance[143] and Okita who defines digital identity as a "collection of claims attached to a digital subject (about which assertions can then be made)."[144]

---

[136] Italics supplied
[137] Cameron (2005) **n131**
[138] ibid
[139] *Id*
[140] OECD, 'At a Crossroads: "Personhood" and Digital Identity in the Information Society,' STI Working Paper, 2007/7, Information and Communication Technologies, DSTI/DOC (2007) 7.
[141] The Identity Gang, a Working Group of the Identity Commons aims to "support the ongoing conversation about what is needed for a user-centric identity "metasystem" that supports the whole marketplace, especially individuals." See Charter <http://wiki.idcommons.net/Identity_Gang_Charter>
[142] The definition can also be found in the Identity Gang's Lexicon <http://identitygang.org/moin.cgi/Digital_Identity>. The OECD paper however, went a step further and stated that this form of digital identity was a "thing," a man-made thing (an "artifact") that refers to a person, and that is different from such person. OECD (2007) **n140**
[143] Liberty Alliance Project, Liberty Alliance Project Whitepaper: Personal Identity (23 March 2006) <www.projectliberty.org/liberty/content/download/395/2744/file/Personal_Identity.pdf>
[144] C Okita, '(Digital) Identity 2.0,' (October 2007) <http://www.usenix.com/publications/login/2007-10/pdfs/okita.pdf>

The identity as claims concept was explored in relation to Facebook by Zhao, Grasmuck and Martin.[145] They conclude that identity construction on Facebook follows a pattern of claims made by individuals or identity subjects, ranging from the implicit to the explicit. Implicit claims were connected to visual cues like photos and wall posts. Explicit claims were those connected to the verbal and narrated descriptions of the self.[146]

Though digital identity presents as claims very neatly, viewing digital identity solely as a claims or a set of claims is highly contentious and problematic because it makes some challenging presuppositions: one, that individuals are able to exert that claim; two, that individuals choose to make that assertion, and three, that individuals are able to support and substantiate that assertion (in case of a conflict, as claims are conflicting by nature and success of claims is also dependent on trust).

2.4.3. Data or information

The most basic and primary view of digital identity is that digital identity is representative of digital data[147] relating to an individual. Turkle states that digital identity is a "collection of fragments of either pre-existing or new data about an individual."[148] That digital identity is representative of digital data is also expressed by Windley[149] who defines digital identity as,

> … containing data that uniquely describes a person or thing (called the subject or entity in the language of digital identity) but also contains information about a subject's relationships to other entities[150]

This data includes attributes,[151] preferences and traits of the subject or entity. Attributes include facts like medical history, purchasing behaviour, banking

---

[145] S Zhao, S Grasmuck and J Martin, 'Identity Construction on Facebook: Digital Empowerment in Anchored Relationships,' (2008) 24 (5), Computers in Human Behavior, 1816-1836
[146] Zhao (2008) **n145**, 1824-25
[147] For definition see IC Pyle & V Illingworth (eds), *The Oxford Dictionary of Computing* (OUP, Oxford 1997), 118
[148] S Turkle, *Life on the Screen: Identity in the Age of the Internet* (Simon & Schuster, NY 1995)
[149] Windley (2005) **n122**
[150] Windley (2005) **n122,** 8
[151] Lessig conceptualised digital identity in terms of attributes, which are broadly "all the facts about you… that are true" that are known when communicated, revealed or asserted. L Lessig, *Code: Version 2.0* (Basic Books, NY 2006), 39-40. Pfitzmann and Hansen too define digital identity as "any subset of attributes of an individual person which sufficiently identifies this individual person within

information etc. Preferences are indicative of the subject or entity's desires like meal or dress choices. Traits relate to the inherent features of the subject or entity.[152] This definition of digital identity can be applied across most contexts and schemes of identity and can relate to human beings and well as other entities.[153]

There are also other definitions that fit within this category. Kobelius defines digital identity as "the set of digital information - including user IDs, passwords, access control lists, public-key certificates, and voiceprint patterns - that is associated with a particular individual…"[154] Loncke defines digital identity in similar manner. According to him, digital identity is "digital information that creates the image of an individually identifiable person."[155] Both these definitions present digital identity as digital information connected to individuals.

'Digital identity is data or information associated with an individual' is the predominant view in the Western digital identity discourse and also mirrored in how the law conceptualises digital identity in Europe in privacy, data protection culture and regulation. Digital identity has become rooted in the legal concept of personal data. Personal data is defined by the EU Data Protection Directive,[156] as "any information relating to an identified or identifiable natural person."[157] An identified or identifiable natural person is who "can be identified, directly or indirectly, in

---

any set of persons." A Pfitzmann and M Hansen, 'Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management: A Consolidated Proposal for Terminology,' v0.31, 15 February 2008 <http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf>

[152] Windley (2005) **n122**, 9

[153] Though the scope of the thesis is limited to studying digital identity in relation to the individual, digital identity also applies in the context of non-human entities like animals (Birch 2007 **n122**, xviii), machines or programs (Windley 2005 **n122**, 9), software agents, things, websites (JND Gupta, SK Sharma, MA Rashid, *Handbook of Research on Enterprise Systems* (IGI Global, 2009) and can be used to represent them.

[154] J Kobelius, quoted by D Costa, 'Identity Crisis,' PC Magazine, 15 October 2002, <http://www.pcmag.com/print_article2/0,1217,a=31229,00.asp>

[155] M Loncke, 'Identity: A Legal Perspective,' FIDIS WP2 Workshop, 2-3 December 2003.

[156] Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (***The Data Protection Directive***), OJ L 281, 23 November 1995, 0031 - 0050

[157] Article 2 (a)

particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." [158]

The Article 29 Working Party paper on personal data,[159] based on national Europe wide practices of data protection authorities, sheds light on what constitutes personal data.[160] It elaborates that the concept of personal data under the Data Protection Directive is a broad one and providing all requirements are met includes,

> information available in whatever form, be it alphabetical, numerical, graphical, photographical or acoustic, for example. It includes information kept on paper, as well as information stored in a computer memory by means of binary code, or on a videotape, for instance.[161]

Examples of personal data are: sound or image data, taped recordings of customer's banking instructions, recognizable CCTV images of people, data in RFID chipped passports and IP addresses.[162]

In the UK, the Data Protection Act 1998 (DPA 1998), Part I, section 1 defines "personal data" as data relating to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.[163]

But, unlike the EU and UK regimes, there is no established concept of digital identity as an individual's personal data in India, even though the concepts of data,

---

[158] Article 2 (a)
[159] Opinion 4/2007 on the Concept of Personal Data. Adopted on 20 June 2007, 01248/07/EN, WP 136
[160] The objective of the above opinion was "to come to a common understanding of the concept of personal data, the situations in which national data protection legislation should be applied, and the way it should be applied."
[161] Opinion 4/2007, **n159**
[162] For an analysis of personal data, see S Booth and others, 'What are 'Personal Data'? A Study Conducted for the UK Information Commissioner,' 2004, <http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/executive_summary.pdf>
[163] For guidance on what constitutes personal data under the DPA1998, see ICO, 'Data Protection Technical Guidance: Determining What is Personal Data,' (2007), <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf>

information and sensitive personal data are embodied in the Information Technology Act 2000 (ITA 2000) as amended by the Information Technology Amendment Act 2008 (ITAA 2008) and are representative of digital identity. Data is defined by the Act, Chapter I, section 2 (o) as,

> a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer

Information, according to the Act, Chapter I, section 2(v), includes, "data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche." Sensitive personal data, is not specifically defined but simply clarified in Section 43A (iii) as referring to "such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit." Here we see the contrast in the UK and Indian positions on personal data.

2.4.4. Identifiers

Digital identity may also present itself in the form of identifiers. An identifier is a sign, token, value or symbol that represents identity. An identifier points to a person or entity[164] or singles that person or entity out from another.

The most universal and common example of an identifier is a name. Names[165] are the most important aspects, sources and heralders of identity, both digital and non-digital. Even the law recognises this position.[166] Names are crucial aspects of and mandatory on most legal documents like passports, ID cards, residence certificates, contracts, wage slips, bank statements and other like documents. Names are much

[164] OECD (2007) **n140**

[165] According to the Oxford English Dictionary, the "individual designation by which a particular person or thing is known, referred to, or addressed."

[166] Names are also a much litigated subject in the ECtHR. See *Burghartz v Switzerland* (1994) 18 EHRR 101; *Stjerna v Finland* 24 EHRR 195 (1994); *Case of L v Lithuania* ECtHR, App 27527/03, (11 September 2007); *Daróczy v Hungary* ECtHR, App 44378/05 (1 July 2008)

favoured options in identifying people as opposed to number based identification (an approach that was even favoured by the UNCRC Human Rights Committee who stated in their comments that "providing for the right to have a name is of special importance."[167] Names, personal and non-personal, are a significant digital identifier and serve a two fold purpose: communication and identification.[168] In the digital identity context, one could be automatically assigned a name, create a name or assume a name.

But names are not the only form of digital identifiers. Numbers, codes, digital tags and tokens are other examples of digital identifiers. The DPA 1998 mentions identifiers in relation to personal data. A general identifier is defined as any identifier (e.g., a number or a code that is used for identification purposes) that relates to an individual and forms a part of a set of similar identifiers which is of general application.[169] For instance, a tag on a photo that names and distinguishes the individuals in the photo is an identifier.

Identifiers may work by themselves or in conjunction with other identifiers to identify an individual. There may also be more than one or multiple identifiers for a single individual. While this can be advantageous, it also is perceived to be problematic from the management and regulatory perspectives.

2.4.5. Presence

Digital presence, particularly in respect of behaviour and location is another potent form of digital identity.

An individual's digital behaviour is representative of digital identity. David Berlind states, "everything you put on the Internet is an expression of your identity."[170] This statement though extremely wide, to a large extent holds true. Even in the non-digital

---

[167] In reference to children born out of wedlock. UN Human Rights Committee, General Comment 17, 1989, HRI/GEN/1/Rev.5, 133

[168] S Bechtold, 'Governance in Namespaces,' (2003) 36 Loyola of LA L Rev, 1248; RJ Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (Wiley, NY 2001), 125

[169] Sch 1, Part II, 4 (2)

[170] Quoted by Andy Oram, 'The Long View of Identity,' *O'Reilly*, 29 June 2006, <http://onlamp.com/pub/a/onlamp/2006/06/29/the-long-view-of-identity.html?page=1>

context, the relationship between behaviour and identity is well established.[171] For instance, behaving kindly would lead a person to be identified as a kind or charitable person. Similarly, stealing would lead to a person being branded a thief.

Digital identity is, moreover, tied to digital behaviour. One's digital identity may manifest as a chat room sexual fantasist, environmentalist Tweeter, a sword wielding Avatar or a Farmer on Farmville.[172] Digital behaviour, as digital identity has social and legal consequences and is employed for various purposes like profiling,[173] behavioural targeting[174] and marketing.

In a wide sense, every action taken by a digital subject in the digital world is indicative of a digital identity subject's behaviour and consequently leads to a development and pinning down of that subject's identity. Depending on what one does, the websites one visits, the items one purchases, with whom one banks, where holidays are taken, search terms are used, a comprehensive personality (or profile) of the individual can be built up. An example is the profiling of online consumer behaviour.[175]

Another aspect of digital presence is location. Digital identity also manifests itself in the form of location data. Location data are data capable of indicating the geographical position of a device or person.[176] Location based digital identities are

---

[171] S Stryker, 'Identity Salience and Role Performance: The Importance of Symbolic Interaction Theory for Family Research,' (1968) 30 J Marriage and the Family, 558–564; S Stryker, *Symbolic Interactionism: A Social Structural Version* (Blackburn Press, West Caldwell 2002); CJ Armitage and M Conner, The Theory of Planned Behaviour: Assessment of Predictive Validity and Perceived Control,' (1999) 38 Brit J of Soc Psych, 35–54; PL Callero, JA Howard and JA Piliavin, 'Role Identity and Reasoned Action in the Prediction of Repeated Behaviour,' (1987) 50 Soc Psych Q, 247–256;

[172]<http://www.farmville.com/>

[173] M Hildebrandt, 'Profiling and the Identity of the European Citizen' in M Hildebrandt, S Gutwirth (eds), *Profiling the European Citizen: Cross-disciplinary Perspectives,* (Springer, Netherlands 2008), 303-344

[174] Alice Klever, *Behavioural Targeting: An Online Analysis for Efficient Media Planning?* (Diplomica Verlag GmbH, Hamburg 2009)

[175] S Karas, 'Privacy, Identity, Databases,' (2002) 52 Am U L Rev, 394-445, 426-427

[176] Location data is defined in The Data Retention (EC Directive) Regulations 2009, s 2 (d)

perpetuated by location-based devices like mobiles and PDA's.[177] These digital identities are becoming increasingly popular and socially and legally significant.[178] Take for instance the growth of geotagging.[179]

2.4.6. Relationship representations

Identity is a representation of relationships.[180] Relationships constitute identity and give it its meaning. For instance, I am who my family is. I am who my friends are. I am who I work for. I am who I communicate and associate with. The relationships of digital identity subject enable the building of digital profiles, sociological or otherwise of the subject. Conversely, they also affect adversely the creation and enjoyment of digital identity. This is an identity aspect of great significance in relation to India.

In the digital context, relationship based identity is best illustrated by the Friend of a Friend (FoAF) concept; defined as the Resource Description Framework (RDF) vocabulary a digital identity subject uses to make statements about itself and its digital identity.[181] It permits the building of web of acquaintances.[182] This is evidenced in Typepad[183] and LiveJournal.[184]

---

[177] E Paulos and E Goodman, 'The Familiar Stranger: Anxiety, Comfort and Play in Public Places,' Proceedings of the Conference on Human Factors and Computing Systems, CHI 2004, Vienna, 24-29 April 2004.

[178] R Clarke and M Wigan,'You are Where You've Been: Location Technologies' Deep Privacy Impact,' in K Michael & MG Michael (eds), *Australia and the New Technologies: Evidence Based Policy in Public Administration* (University of Wollongong, 2008), 100-113

[179] See Gene Smith, *Tagging: People-Powered Metadata for the Social Web* (New Riders, Berkeley 2008),111; 'Foursquare Roads to 3 Million Users,' *ABH News*, 31 August 2010 <http://abh-news.com/foursquare-roads-to-3-million-users-4049.html>

[180] S Chen, HC Boucher and MW Kraus, 'The Relational Self: Emerging Theory and Evidence,' in VLVignoles, S Schwartz and K Luyckx (eds), *Handbook of Identity Theory and Research* (Springer, NY 2011); SM Andersen, S Chen and R Miranda, 'Significant Others and the Self, (2001) 1 Self & Identity,159-168

[181] Erle Schuyler, Rich Gibson and Jo Walsh, *Mapping Hacks: Tips and Tools for Electronic Cartography* (O'Reilly Media, CA 2005), 503

[182] Kieron O'Hara and Nigel Shadbolt, 'Knowledge Technologies and the Semantic Web,' in R Mansell and BS Collins (eds), *Trust and Crime in Information Societies* (Edward Elgar, UK 2007), 113-164, 134

[183] <www.typepad.com>

[184] <www.livejournal.com>; Schuyler (2005) **n181,** 503

2.4.7. Reputation

Digital identity may also take the form of reputation. Reputation is a key component of identity and identity is often the summed up in terms of reputation. This kind of identity is particularly important in close knit communal and collective cultures like India.[185]

Reputation is a vital and significant digital identity component. It is important not just in the online context but also in the offline context. The Internet through search engines enables the aggregation and assimilation of an individual's reputation, as do digital databases used to collate personal information and build profiles.

Reputation is the "overall quality or character as seen or judged by people in general," or the "recognition by other people of some characteristic or ability."[186] Reputation can be positive or negative. Negative reputation can be developed by telling or posting true or false stories or allegations about individuals.[187] For instance, posting defamatory messages in newsgroups[188] or indulging in name-calling on message boards.[189] There are specialist reputation building sites like Rotten Neighbour,[190] (permits the posting of information about good and bad neighbours), RateMyTeachers,[191] (site for rating teachers) etc. A disreputable digital identity can have serious consequences. For instance, non-consideration for employment. Such problems have resulted in the growth of reputation management services.[192]

---

[185] In India, often classified as a high context culture, reputation plays a significant role particularly given close knit nature of interpersonal bonds. Brian Black, *The Character of the Self in Ancient India: Priests, Kings, and Women in the Early Upanisads* (SUNY, Albany 2007), 83 (losing reputation is a terrible consequence); MV Sidhpuria, *Retail Franchising* (Tata McGraw Hill: New Delhi 2009), 120 (high reliance placed on reputations in transactions); Mattison Mines, *Public Faces, Private Voices: Community and Individuality in South India* (University of California Press, California 1994), 6, 32 (reputation as crucial in life negotiation)

[186] See Merriam Webster Inc, *The Merriam-Webster Dictionary* (Merriam Webster, Springfield MA 2005)

[187] See 'Business Rival Makes Highest Ever Online Libel Payout,' *Out-LAW News*, 3 April 2008, <http://www.out-law.com/page-9011>

[188] *Godfrey v Demon Internet Limited* [2001] QB 201

[189] <http://www.guardian.co.uk/media/2006/mar/23/digitalmedia.law>

[190] <http://www.rottenneighbor.com/>

[191] <http://uk.ratemyteachers.com/>

[192] For instance, Garlik. <www.garlik.com>

Reputation systems too, have proliferated on the Internet.[193] Dellarocas states the Internet based reputation systems differ from non-Internet based in the following three aspects: their unprecedented scale;[194] the ability of their designers to precisely control and monitor their operation through automated feedback mediators; and the new challenges introduced by the unique properties of online interaction, like the volatile nature of online identities[195] and the near complete absence of contextual cues.[196]

On EBay, buyers and sellers rate one another. Transactions occur on the basis of the reputational identities of the participants. In virtual world games like WoW, reputation is central to being able to undertake quests and make purchases as required in the game.[197]

Reputation is also constructed on offline databases by the aggregation of digitally compiled data about a digital identity subject. This reputation is constructed and develops as a result of data collection and storage, and use in private and government databases. For example, in the UK this is evident in Police National Computer (PNC)[198] (convicted offenders), Youth Offender Information System (YOIS) system[199] and the National Pupil Database.[200] In India, it is evident in the National Skills Registry.[201]

---

[193] P Resnick, R Zeckhauser, E Friedman and K Kuwabara, 'Reputation Systems,' (2000) 43 (12) Communications of the ACM, 45-48

[194] Internet reputation transcends geographical boundaries. Edwards refers to this as the bounced or exploding out effect. L Edwards, 'Defamation and the Internet: Name Calling in Cyberspace,' in L Edwards and C Waelde (eds), *Law and the Internet: Regulating Cyberspace* (Hart Publishing, Oxford 1997), 183-198

[195] E Friedman and P Resnick, 'The Social Cost of Cheap Pseudonyms,' (2001) 10 (1) J Eco and Mgt Strategy, 173-199.

[196] C Dellarocas, 'The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms,' (2003) 49 (10) Management Science, 1407-1424

[197] <http://www.worldofwarcraft.com/info/basics/reputation.html>

[198] NPIA Police National Computer, <http://www.npia.police.uk/en/10508.htm>

[199] <http://www.socialsoftware.co.uk/Development/172.asp>

[200] This database stores information on pupils' behaviour, attendance records, and talents.

[201] <https://nationalskillsregistry.com>. The National Skills Registry, a NASSCOM initiative, aims at facilitating the development of credible, permanent and accessible information about registered persons from the IT industry.

The above examination reveals how digital identity can assume different forms: authenticators, claims, data or information, identifiers, presence, representation of relationships or reputation. Any or all of these singly or in combinations of various sorts could represent a digital identity subject's identity. These may vary according to context and across domains.

2.5. Nature of digital identity

This section now explores the nature of digital identity. Given that digital identity is represented in various forms, the character of digital identity is now explored.[202]

2.5.1. Unitary or multiple

I am one. I am many.

A digital identity can be of unitary or multiple nature. A unitary digital identity is an identity that stands by itself. The post-modern[203] era is characterised by focus on the multiplicity of identities.[204] But multiple identities are not a new occurrence specific to the development and proliferation of digital technologies, as highlighted by the works of Goffman,[205] Gergen,[206] Kendall[207] and Poster.[208]

---

[202] The properties of identity were also explored in OECD (2007) **n140**.

[203] Postmodernism is defined as "a set of critical, strategic and rhetorical practices employing concepts such as difference, repetition, the trace, the simulacrum, and hyper reality to destabilize other concepts such as presence, identity, historical progress, epistemic certainty and the univocity of meaning." Gary Aylesworth, 'Postmodernism,' The Stanford Encyclopedia of Philosophy, (2005), <http://plato.stanford.edu/entries/postmodernism/>.The postmodern is embodied in the works of G Bennington and Brian Massumi (trs), *JF Lyotard: The Postmodern Condition: A Report on Knowledge*, (University of Minnesota Press, Minneapolis 1984); Richard Howard (tr), *Michel Foucault:Madness and Civilization: A History of Insanity in the Age of Reason* (Random House, NY 1965); Robert Hurley (tr), *Michel Foucault:* The *Use of Pleasure: The History of Sexuality, Vol Two* (Random House NY 1985); Hugh Tomlinson (tr), *Nietzsche and Philosophy: Gilles Deleuze* (Columbia University Press, NY 1983); GC Spivak (tr), *Jacques Derrida of Grammatology* (Johns Hopkins University Press, Baltimore 1974); IH Grant (tr), *Jean Baudrillard, Symbolic Exchange and Death* (Sage, London 1993); JR Snyder (tr), *Gianni Vattimo, The End of Modernity: Nihilism and Hermeneutics in Postmodern Culture* (Johns Hopkins University Press, Baltimore 1988); Christopher Woodall (tr), *Mario Perniola, Enigmas: The Egyptian Moment in Society and Art* (Verso, London 1995)

[204] Eg Diana Fuss, *Essentially Speaking: Feminism, Nature and Difference* (Routledge, NY 1989), p 98, 99; M Rosenthal, 'What was Postmodernism,' (1992) 22 (3) Soc Rev, 83-105, 96

[205] Goffman (1959) **n100**; Erving Goffman, *Stigma: Notes on the Management of Spoiled Identity* (Simon and Schuster, NY 1963)

[206] KJ Gergen, *The Saturated Self: Dilemmas of Identity in Contemporary Life* (Basic Books, NY 1991)

[207] L Kendall, 'Recontextualizing 'Cyberspace: Methodological Considerations for On-Line Research,' in S Jones (ed), *Doing Internet Research: Critical Issues and Methods for Examining the Net* (Sage, California 1999), 57-74, 61

[208] M Poster, *The Mode of Information: Post-Structuralism and Social Context* (Polity Press, Cambridge 1990), 6

Individuals may adopt any number of digital identities, technology and law permitting.[209] They have, as Turkle suggests, "the chance to express multiple and often unexplored aspects of the self, to play with their identity and to try out new ones."[210] Individuals can have and express a myriad of digital identities across technical platforms like the computer, Internet, mobile phones. They can use these identities to work across contexts and enter and exit different worlds simultaneously.[211]

Turkle makes the case that digital identity subjects view their identity as multiple and incorporated at the same time.[212] This is supported by Kendall's research and her conclusion that "people persist in seeking essentialised groundings" and "continually work to reincorporate their experiences of themselves and of other selves into integrated, consistent wholes."[213]

Even in the non-digital context, people have and assume different identities – constantly moving in and out of them as a matter of routine. In similar vein to Turkle, Waskul and Douglas conclude that multiple digital identities are influenced by the Internet's potential of dislocating and disembodying identities, and "exposing the hyper fluidity of self-enactment."[214] Stone, another post-modern theorist, talks about the how the "mode of computer nets" suggests "fragmentation and multiplicity as an integral part of social identity."[215]

The multiplicity of identities is a key feature of virtual worlds[216] (including MMORPGs and MMORLGs). The use of services from multiple web providers (for

---

[209] H Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier* (Addison Wesley: Mass 1993), 147 (MUD personas)
[210] Turkle (1995) **n148,** 12
[211] Turkle (1995) **n148**, 13
[212] S Turkle, 'Computational Technologies and Images of the Self,' (1997) 64 (3) Social Research, 1094-1111, 1103-1105
[213] Kendall (1999) **n207**, 62
[214] D Waskul and M Douglas, 'Cyberself: The Emergence of the Self in On-line Chat,' (1997) 13(4) The Information Society, 375-397, 394
[215] A Stone, 'Virtual Systems,' in J Crary and SK Winter (eds) *Zone 6: Incorporations* (MIT Press, Mass 1992), 609-621, 611
[216] DT Nguyen and J Alexander, 'The Coming of Cyberspacetime and the End of Reality,' in R Shields (ed), *Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies* (Sage, London 1996), 99-124

different purposes) also results in multiple identities. A Security Report on Online Identity Theft reports that a single person could legitimately have around 15-20 digital identities for different purposes and in different contexts.[217] For instance, a person might have three email accounts, four social networking profiles, one PayPal account, an Amazon account and three avatars in three different domains.

The multiplicity of digital identities has been viewed of as a problem by identity technologists and law. Identity technologists developed identity management solutions (outlined in Chapter 4) to help control and manage multiple identities. Multiple digital identities are also perceived as a legal regulatory challenge. This is due to the belief that multiple digital identities enable individuals expressing them to escape accountability by moving and hiding between identities,[218] their complex nature and security challenges. They are often associated with criminality. Thus, the law seeks to regulate their exercise. For instance, sex offenders in the State of New York, if legal measures were successfully enacted, would have to register all their digital identities with the police as conditions of their probation or parole. [219]

To control multiple identities, the law often resorts to bolstering the concept of 'one true identity' by rolling out unique identity based governance systems, as was the case in the UK[220] and is in India, [221] revealing a trend disfavouring multiple identities. But the vitality of the multiplicity is still recognised in many circles.[222]

---

[217] BT, 'Security Report: Online Identity Theft,' February 2006, <http://www.btplc.com/onlineidtheft/onlineidtheft.pdf>

[218] T Nabeth, 'Privacy in the Context of Digital Social Environments: A Cyber-Sociological Perspective,' INSEAD CALT-FIDIS Working Paper, (2005); danah Boyd, 'Sexing the Internet: Reflections on the Role of Identification in Online Communities,' Presented at 'Sexualities, Medias, Technologies,' University of Surrey (21-22 June 2001), 10; Esther Dyson, 'Digital Identity Management,' Release 1.0, 20 (6) (28 June 2002), 12

[219] Out-Law News, US Sex offenders to Be Banned from Social Networking for the First Time,' (13 February 2008), <http://www.out-law.com/page-8870>

[220] See House of Commons Science and Technology Committee, 'Identity Card Technologies: Scientific Advice, Risk and Evidence,' HC 1032, Sixth Report of Session 2005-06 (TSO: UK 2006); Home Office, 'Legislation on Identity Cards: A Consultation,' CM 6178, (TSO, UK 2004)

[221] Sebastian Pt, 'The Card Trick,' *Outlook Business* (3 May 2008), 32-34, 34

[222] G Roussos, D Peterson and U Patel, 'Mobile Identity Management: An Enacted View,' (2003) 8 Intl J Elec Commerce, 81-100. In the Indian context, attempts to reduce identity to a singular form have been criticised. See D Anand, 'Security Bites: Political Violence and Identity Construction in India,' International Studies Association Annual Conference (Hawaii, March 2005); M Kishwar, 'Who Am I? Living Identities vs. Acquired Ones,' Revised Version of Keynote Address, UNHCR and AIW Conference on 'Women in Search of Identity' (March 1996) <http://www.infinityfoundation.com/mandala/s_es/s_es_kishw_who_frameset.htm>; R Wilton, 'Racingsnake, The Blog of Future Identity: Is Privacy only for the Rich?' Blogpost (11 March 2009)

2.5.2. Same or different

I am 'that' one. I am not 'that' one.

A digital identity may or may not relate to its digital identity subject. This means a digital identity might embody the characteristics of the digital identity subject, [223] or alternately, it may take on different characteristics in comparison with the characteristics of the digital identity subject. [224]

For instance, X X is X X on Facebook. However, X Y is X Z on LiveJournal. A middle aged male psychiatrist might pose as a disabled woman.[225] A man may present himself as a woman. A 45 year old might pretend to be a 16 year old. A survey of 9,529 Second Lifers, showed how 45 percent of respondents gave their avatars more attractive bodies than they actually had, 37 percent made themselves younger and 23 percent chose a different race. [226]

2.5.3. Fixed or flexible

I am unchanging. I am dynamic.

Digital identity may be fixed or flexible in nature. The fixed nature of digital identity manifests itself in its embodiment in rigid, unchangeable form due to its own, technical, legal or other constraints. Flexible digital identity is dynamic and non-resistant to alteration. [227]

One example of a fixed digital identity is a biometric identifier like a digital fingerprint. A digital fingerprint relates to an individual and generally remains the same over time and place for that individual. Another example is a permanent lifelong ID token issued by an authority intended to represent a digital identity subject e.g. the UK national insurance card and the Indian UID card. Fixed digital

---

[223] See MG Kirschenbaum, 'Why I Blog Under My Own Name (and a Modest Proposal),' (9 July 2005) <http://www.otal.umd.edu/~mgk/blog/archives/000813.html>

[224] Goffman (1963) **n205**

[225] See AR Stone, 'Will the Real Body Please Stand Up? Boundary Stories about Virtual Cultures," in D Bell, BM Kennedy (eds), *The Cybercultures Reader* (Routledge, London 2000), 504-528, 506

[226] JH Burnett, *MiamiHerald* <http://www.weblo.com/mediacenter/media/More-People-are-Leading-Virtual-Lives_Miami-Herald.pdf>

[227] For flexibility of identity in communication networks see: Lee Sproull and Sara Kiesler, 'Reducing Social Context Cues: Electronic Mail in Organizational Communication,' (1986) 32 Management Science, 1492-1512; Lindsay Van Gelder, 'The Strange Case of the Electronic Lover,' in Gary Gumpert and SL Fish (eds), *Talking to Strangers: Mediated Therapeutic Communication* (Ablex, Norwood 1990), 128-142

identities fixate the identity of the digital identity subject. The digital identity subject might or might not have a say in such a fixation, particularly in cases where such identities are not created or subject to the operative control of the digital identity subject.

Fixed identities are subject to the problems and issues like inertia, redundancy, inaccuracy development, irrelevance, irreversibility and ease and susceptibility to compromise and abuse.[228]

Flexibility of digital identity manifests in the ability of a digital identity subject to play with their identity.[229] Some digital identities lend well to moulding and adaptation in different manners, as in the case of Avatars.[230] Subject to the terms of the operating platform, an Avatar is free to assume any form (i.e. animal, human, part human, part animal, male, female, abstract or concrete). Avatars can change between forms and appearances at will.[231]

2.5.4. Local or universal

I am here. I am everywhere.

Digital identity may be local, universal or simultaneously both. In relation to the Internet, Buchanan states that one may be "simultaneously everywhere and nowhere."[232] In similar light, Poster comments,

> … we are being changed from "arborial" beings, rooted in time and space, to "rhizomic" nomads who daily wander at will (whose will remains a question) across the globe, and even beyond it through communications satellites,

---

[228] This emerges particularly in the arguments against genetic biobanks. See SB Haga and LM Beskow, 'Ethical, Legal and Social Implications of Biobanks for Genetics Research,' (2008) 60 Advances in Genetics, 505-544; JH Solbakk, S Holm and B Hofmann, *The Ethics of Research Biobanking* (Springer Verlag, NY 2009)

[229] SL Calvert, 'Identity Construction on the Internet' in SL Calvert, AB Jordan and RR Cocking (eds) *Children in the Digital Age: Influences of Electronic Media on Development* (Praeger, Westport 2002), 57-70

[230] JA Bryant and Anna Akerman, 'Finding Mii: Virtual Social Identity and the Young Consumer,' in NT Wood and MR Solomon (eds), *Virtual Social Identity and Consumer Behavior* (ME Sharp Inc, USA 2009)

[231] M Fowle, 'Interdentity: Belonging, Behaviour and Identity Online,' Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (19-25 February 2006)

[232] J Buchanan, 'Beyond East and West: Postmodern Democracy in a Mode of Information,' in R Bontekoe & M Stephaniants (eds), *Justice and Democracy: Cross-Cultural Perspectives* (University of Honolulu Press, Honolulu 1997), 423

> without necessarily moving our bodies at all. The body then is no longer an effective limit of the subject's position.[233]

Poster further poses the question, "then where am I and who am I?" and concludes with the rejoinder that "I am disrupted, subverted and dispersed across social space."[234] Contemporary digital space and identity thus, knows few geographical boundaries.

Digital identity has both local and universal dimensions. A simple example illustrates this. Shanta accesses the Internet through a computer in a cybercafé in Trivandrum, India. She has a Facebook profile, which is available to her locally as well as available to her friends all over the world. Thus her profile, is local and yet universal in nature. Another example is of a biometric passport. A biometric passport may issued by the government of India and yet valid in other countries across the world.

Yet, though the technologies of identity seem to have the capacity to enable both local and universal expression of digital identity, they are constrained by local differences in the use, experience[235] and regulation of these technologies. [236]

2.5.5. Authentic or fictitious

I am true. I am false.

A digital identity may be authentic or fictitious. Authentic digital identities are digital identities that are established or confirmed as true in relation to a digital identity subject. Fictitious digital identities are the opposite.

Digital identities have a propensity for fictitiousness.[237] Raab states that, "in a post-modern world, it is no longer clear that any one identity is real."[238] Fictitiousness

---

[233] Poster (1990) **n208**, 1-16
[234] Poster (1990) **n208**, 15-16; Also M Poster, *The Second Media Age* (Polity Press, Cambridge 1995), 59
[235] Substantiated in **Ch 3**
[236] Comprehensively addressed in **Chs 4 & 5**.
[237] A Vasalou and AN Joinson, 'Me, Myself and I: The Role of Interactional Context on Self-Presentation Through Avatars,' (2009) 25 (2), Comput Hum Behav, 510-520
[238] Charles Raab, Keynote Address, Proceedings of the Life of Mobile Data, University of Surrey, Guildford (April 2004)

might manifest in digital identities that seem fake or unreal. In virtual worlds there is a wide-ranging possibility to enact fantasy [239] and create fantasial or fictitious identities.

Identities may fictionalised for any number of reasons: to express oneself (especially in terms of breaking offline restrictive boundaries),[240] for privacy or anonymity.[241] A blogger may adopt a fictitious identity to voice concern over politically sensitive issues. A Twitter user may adopt a fictitious identity and lurk on Twitter to follow issues relating to medical conditions. A twelve year old might adopt a fake adult identity and log onto adult websites.

Authenticity of digital identity can be established or confirmed by determining whether a digital identity in relation to a digital identity subject is what it is, claims to be, or is connected or related to the digital identity subject in some form or manner. If it is not, then it is fictitious. Fictitious digital identities create law enforcement problems, as they are difficult to control, particularly if they cannot be traced back to a digital identity subject.[242] While fictitious identities are not illegal in themselves, their use for illegal purposes is generally proscribed by law.

2.5.6. Possessed or owned

I am mine, but not my own. I am my own.

Digital identity might be subject to possession or ownership by a digital identity subject. Alternately, a digital identity subject might have both possession and ownership. If a digital identity subject only possesses a digital identity, ownership might lie elsewhere (e.g. in the case of an issued identity token, with the identity provider).

---

[239] Turkle (1995) **n148***;* see also HJ Schau & MC Gilly, 'We Are What We Post? Self-Presentation in Personal Web Space,' (2003) 30 (3) J Cons Res, 385-414

[240] JP Gee, *What Video Games Have to Teach Us About Learning and Literacy* (Palgrave Macmillan, NY 2003)

[241] Dorian Wiszniewski and Richard Coyne, 'Mask and Identity: The Hermeneutics of Self-Construction in the Information Age,' in KA Renninger and Wesley Shumar (eds) *Building Virtual Communities* (Cambridge Press, NY 2002), 191-214

[242] DJ Solove, M Rotenberg and PM Schwartz, *Privacy, Information and Technology* (Aspen Publishers, NY 2008); GP Schneider, *Electronic Commerce* (Course Technology, Canada 2009); LE Bone, DL Kurtz, *Contemporary Business* (Wiley, 2003)

Digital identity is contentious in relation to who "owns" it.[243] Here is an example to illustrate this: Tom has an email account with Moyi, an email provider. Though Tom has actual possession of his email id (with access to its use with a username and password), Tom does not own his digital identity, even though it relates to him and he is the sole user of his email account.

There are many more examples of this kind. For instance, while one may control one's Yahoo id!, one cannot "reproduce, duplicate, copy, sell, trade, resell or exploit for any commercial purposes, any portion or use of, or access to, the Yahoo! Services (including Content, advertisements, Software and your Yahoo! ID)."[244] Where ownership lies, clearly vests in the clause that states "You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted."[245] Many other digital identity services have similar terms and conditions that vest ownership of digital identity with the identity provider.[246] Even in OpenId,[247] a free platform that enables the use of a single digital identity across the Internet, the core identity, though relating to and possessed by the digital identity subject, is not owned by it. Similarly, WoW characters are owned by Blizzard, not players.[248]

It is thus evident that while a digital identity may relate, identify or pertain to an identity subject, the identity in question may not belong to the identity subject. The identity subject may not have ownership in the very identity he identifies with, relates to or inhabits.

---

[243] Halstead-Nussloch highlights international differences in attitudes in this respect, contrasting practice in the US where "possession is nine-tenths of the law with respect to digital identity and data from personalisation" and Europe where "person whose digital identity has been digitized is given the nod of ownership." Richard Halstead-Nussloch, 'Self-Service, Personalization and Electronic Government,' in Clare-Marie Karat, JO Blom and J Karat (eds), *Designing Personalized User Experiences in E-Commerce* (Springer-Verlag, NY 2004), 161-184, 176

[244] Yahoo! Terms of Service, 12 <http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html>

[245] ibid, 27

[246] See Google Terms of Service for Orkut < http://www.orkut.com/html/en-US/additionalterms.orkut.html>

[247] <http://openid.net/>

[248] WoW, Terms of Use Agreement, Terms 7 & 11

2.5.7. Assigned or assumed

I am what I am given. I am what I choose to be.

Identity is often a product of what is given to or associated with us by other individuals, groups or entities. For example, names and identity numbers. Identity may also be something that an individual chooses for oneself. For instance, profession, place of residence, memberships of associations and clubs etc. In similar fashion, digital identities may be assigned identities or assumed identities.

A large segment of digital identities are assigned identities; identities that are given to digital identity subjects by other entities. For example, smart cards and user account identities. But there are also digital identities that an individual may itself assume – like a particular Avatar form or specific profile picture. Assigned and assumed digital identities may not always function exclusively of each other. Many a times, they increasingly interact and interpose upon one another.

2.5.8. Fragmented or cohesive

I am dispersed. I am integrated.

Digital identity may be fragmented or cohesive.

The very nature of the Internet and condition of digital technology lends well to the fragmentation of digital identities. A digital identity subject can have numerous coordinated or uncoordinated digital identities all representing elements and narratives of itself, both online and offline. These are piecemeal and can even be incoherent narratives of an individual.

There is increasing evidence of resistance of identity fragmentation. Identity fragmentation and proliferation are visualised as problems, particularly in regards to identity management and regulation.[249] For instance, fragmentation of digital identities is often associated with the falsification of identities.[250] SSO and Federated

[249] Fragmented identities, like multiple identities, are associated with confusion, discontinuity, conflict, management problems. See **Ch 4 (4.2)**

[250] ITU Internet Report 2006, 'Digital.Life,' Chapter 4, <http://www.itu.int/osg/spu/publications/digitalife/docs/digital.life-chapter4.pdf>

Identity Management[251] are evidence to a certain extent of the fact that fragmented identities were perceived as a regulatory difficulty.

Digital identity may also be cohesive or integrated. Cohesive identities are an amalgamation of the identities of a digital identity subject. Here, a single platform embodies multiple identity elements of a digital identity subject. Social networking profiles to some extent are examples of cohesive or integrated identity. These profiles are an amalgamation of personal, professional and social identity.

2.5.9. Public or private

I am public. I am private.

Digital identity may be public or private. Public digital identities are digital identities that are within the public realm. Private digital identities are digital identities that are largely within the private sphere.

Public digital identities are open and shared digital identities. The digital identity in this case is one that is widely, easily and freely available to anyone who wishes to avail of it or access it. Examples of public digital identity are publicly available digital information (like names), public profiles, domain names, digital images or reputation.

Private digital identity relates to digital identity that is limited in terms of its access. These identities are actively subject to measures that limit them from being exposed to the public realm. The access and knowledge of these identities is limited to the identity subject, the identity provider and/or the service provider, or by agreement between a limited number of entities who share specific relationships. Some examples of private digital identities might be passwords, financial data, medical or biometric data.

Digital identity subjects can sometimes make a choice (as per their expectations and requirements) as to whether they wish their digital identities to be public or private.

[251] See **Ch 4**

This is evident in the mediation of digital identity on social networking websites. These sites allow digital identity subjects to restrict access to their digital identity with specific tools designed for the purpose. For instance, a Facebook user may chose who has access to their profile, block people from accessing their profile and determine what parts of their profile are open and what parts are closed.

2.5.10. Anonymous or pseudonymous

I am …. I am X.

Anonymity refers to the condition of being unable to ascertain or determine identity or origin. A digital identity is anonymous when it cannot be linked to an entity or its user.[252] Clarke defines an anonymous identity as one that "cannot be associated with a particular individual, either from the data itself, or by combining the transaction with other data."[253]

A pseudonymous identity[254] is "one that cannot**,** in the normal course of events*,* be associated with a particular individual.*"*[255] It represents an identity that is in between anonymity and complete identification. A digital identity is pseudonymous[256] if it can be linked to its entity or user if certain other conditions are fulfilled (e.g. user generated public keys).

Contemporary digital identities are not, contrary to popular belief, anonymous. A person may seek to shield or hide their digital identity (by use of platforms like Anonymizer.com,[257] The Cloak,[258] Tor[259] and Privoxy[260] and services like anonymous attribute certificates and signatures), but it can be easily revealed[261] or

---

[252] This form of identity is extinct.
[253] R Clarke, 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice,' User Identification & Privacy Protection Conference, Stockholm (14-15 June 1999)
[254] For overview of pseudonymous identity, see M Mowbray, 'Implementing Pseudonymity' (2006) 3 (1) SCRIPTed 34 <http://www.law.ed.ac.uk/ahrc/script-ed/vol3-1/mowbray.asp
[255] Clarke (1999) **n253**
[256] Pfitzmann and Hansen delve in depth into pseudonyms: Pfitzmann (2008) **n151**
[257] <http://www.anonymizer.com/>
[258] <http://www.the-cloak.com/anonymous-surfing-home.html>
[259] <http://www.torproject.org/>
[260] <http://www.privoxy.org/>
[261] Katherine Walker, 'It's Difficult to Hide It": The Presentation of Self on Internet Home Pages,' (2000) 23 (1) Qualitative Sociology, 99-120

discovered,[262] though it might not be able to be conclusively traced back to the digital identity subject. Identity management systems, though they aim to facilitate anonymity and pseudonymity, through permitting surveillance,[263] symbolise the obsoleteness of the Internet where nobody knows you are a dog.[264]

Anonymous digital identities (and to some extent pseudonymous digital identities to the extent they obscure identity) have become associated with illegal acts like paedophilia, spam, identity crime, defamation, intellectual property theft (e.g. illegal file sharing, copyright infringement) and the commission of other crime and terrorist activities.[265] They are thus resisted, resulting in moves towards enhanced identification of the digital identity subject.

In the digitally advanced West, anonymity and pseudonymity are widely accepted for their liberative potential to an individual's existence,[266] and this explains the development, growth and support for privacy enhancing technologies (PETs). In India however, this is not the perception or case. Culture[267] and legal policy[268] has ensured that digital anonymity and pseudonymity is the exception rather than the rule.

2.5.11. Temporary or permanent

I am fleeting. I am forever.

Digital identities may be temporary or permanent. Transactional digital identities may be temporary i.e. they may be created or last for a session, or couple of sessions. Other digital identities may be longer lasting or permanent, subject to use and re-use. Some digital identities may be time restricted and expire after a certain period

---

[262] Jacob Van Kokswijk, *Digital Ego: Social and Legal Aspects of Virtual Identity* (Eburon, Eindhoven 2007), 221
[263] Further outlined in **Ch 3.**
[264] 'On the Internet, Nobody Knows You're a Dog,' *The New Yorker,* 69 (20), (1993), reprint <http://www.unc.edu/depts/jomc/academics/dri/idog.html>
[265] This is not to negate occurrence of actual harm but to draw attention to the disproportionate nature of the association.
[266] See CEA Karnow, 'The Encrypted Self: Fleshing out the rights of Electronic Personalities,' (1994) 13 JCIL 1
[267] **Ch 3 (3.2.2.6)**
[268] **Ch 6 (6.3.4) & (6.3.5)**

(automatic lapsing) others may be such that they are permanent subject to active revocation or destruction.

It is often very difficult for a digital identity subject to appreciate whether the digital identity or identities in play are temporary or permanent, though the answer to this question would definitely make a difference in the manner they are perceived and dealt with.

Digital identities are quite partial to 'everything lasts forever.' [269] For instance, a person may delete their photo from a blog or social networking site but this may be saved in cache or on another computer. They thus have a propensity to seem temporary, though inherently capable of being permanent in nature. Digital technologies have facilitated and promoted preservation on an unprecedented and even inexpensive scale. This is not always a good thing, particularly for the digital identity subject, because it has serious consequences. [270] This is particularly highlighted by Mayer-Schöenberger who calls for a revival of the social capacity to forget.[271]

2.5.12. Visible or invisible

I am seen. I am unseen.

Digital identities may be visible or invisible in form. Examples of visible digital identities are email ids, avatars, domain names, social networking profiles, chat room handle etc. Examples of invisible digital identities are cookies, digital certificates and embedded identifiers.

A digital identity could also have both characteristics (visibility and invisibility). For instance, reputation could take on both visible and invisible characteristics, to the extent that it is known and unknown (such that the identity subject is not aware it

---

[269] Andy Oram, 'What Sociologist Erving Goffman Could Tell Us About Social Networking and Internet Identity,' O'Reilly Radar (26 October 2009) <http://radar.oreilly.com/2009/10/what-sociologist-erving-goffma.html> (identities as "presented to the entire world for all time")

[270] DJ Solove, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet* (Yale University Press, Newhaven 2007), 33, 94, 165

[271] V Mayer-Schoenberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, NJ 2009)

exists). Even an IP address can be a visible or invisible form of identity depending of the identity subject's knowledge or lack of its existence.

Thus, digital identity has different natures which might exist in isolation, combination to each other. These natures add another layer of complexity to digital identity.

2.6. Digital identity and its relationship to the individual

At the heart of the digital identity lies the digital identity subject - the individual or natural person to whom the digital identity relates to, associates with or represents. This section now examines the relationship of digital identity to the individual.

The relationship of digital identity to an individual can be explained with the help of the Johari window, a graphic model of interpersonal awareness, created by Luft and Ingham.[272] The model gives good insight into the complexity and layers of digital identity.

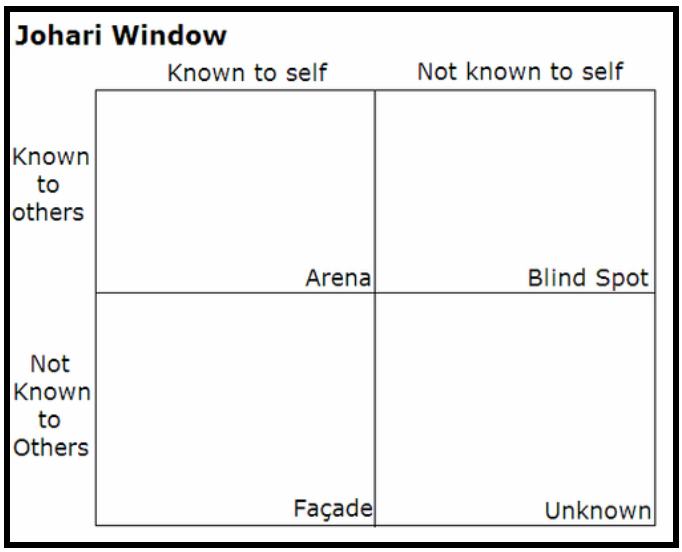

Fig 2: The Johari Window

The Johari window has four aspects to it:

- Known to Self and Known to Others (Arena)

[272] Joseph Luft and Harry Ingham, 'The Johari Window, A Graphic Model of Interpersonal Awareness,' Proceedings of the Western Training Laboratory in Group Development, UCLA, LA (1955)

- Known to Self, Not Known to Others (Façade)
- Known to Others, Not known to self (Blind Spot)
- Not known to self and not known to others (Unknown)

Applying this model to digital identity, we find an individual may have none, one or several digital identities. Some of these digital identities are known to the individual and his associates; these identities fall into the **Arena** category. These digital identities are generally visible and public in nature. For instance, the individual and his friends who he communicates with are aware of the individuals email id, his chat room/IM handle and social networking profile.

An individual also has digital identities that he himself knows about but his digital associates or other persons or entities know nothing about. This may be because the individual needs to keep these secret for security reasons (e.g. passwords, banking id, PayPal id) or it may just be that the individual does not want them to know for reasons like fear of exposure (MMORPG ids), trust betrayal, embarrassment, stigma (e.g. a male creates a female avatar) or for no reason at all. These identities fall into the **Façade** category. More problematic façade identities are fictitious digital identities.

In the **Blind Spot** category are digital identities that others are aware of and the individual is not aware of. For instance, cookies placed on a machine, IP addresses (many users are not aware of their IP address is), DNA profile on a database (uploaded without consent or knowledge). These types of digital identities are problematic in terms of how these digital identity subjects can exercise control over them.

The **Unknown** relates to the collective ignorance of the presence or absence of digital identities. This relates to digital identities that covertly exist but have not yet surfaced - these may be futuristic applications of digital identity.

Different individuals have different relationships with digital identity. As with identity, this relationship is highly subjective. Digital identity subjects bring to their

digital identity their personal, social conditioning and life contexts; specifically in how they use, experience and manage digital identity.[273] This is an important factor to be taken into consideration not just in the context of this thesis but for the regulatory future of digital identity.

In the digitally advanced countries like the UK, individuals to a great extent experience digital identities as crucial and at times inseparable parts of their selves (evident in the disappearance of the distinction between the 'real' and digital identities).[274] This is supported by the European Parliament's Recommendation on the Strengthening Security and Fundamental Freedoms on the Internet which has recognised that digital identity is increasingly becoming an integral part of the self."[275] Digital identity has become a normalised and routine part of life without which life is unthinkable. It is an asset of value[276] to the individual and "people view their personal information to be as valuable as their own cash."[277]

However, in countries like India the position is completely different.[278] There are still distinct fault lines between identity and digital identity and identity and the self, though in some cases identity and digital identity become inevitably connected, either through requirements of the system, policy, law or culture, which influence identity seepage.

---

[273] See **Ch 3**
[274] Birch (2007) **n122**. Birch believes that the boundary between the non-digital (which he terms as the "real") and the digital is unclear and at the same time fascinating for what it means for the emergent concepts of digital identity. And yet, it was important in that people did feel a strong sense of connection between their digital and non-digital identities.
[275] Text adopted on 26 March 2009, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2009-0194>
[276] eg, Kable, 'Identity Management in the UK Public Sector to 2011,' Research Report (July 2007)
[277] M Sparkes, 'Europeans Value Personal Data as Highly as Cash,' (12 October 2007), <http://www.macuser.co.uk/news/129476/europeans-value-personal-data-as-highly-as-cash.html>
[278] R Rodrigues, 'Digital Identity and Anonymity: Desi Manifestations and Regulation,' in S Fischer-Hübner and ors (eds.), *The Future of Identity in the Information Society*, IFIP 262 (Springer, Boston 2008), 359–374

2.7. Conclusion

Digital identity, the digital representation of an individual comes in various shapes and sizes, and in various forms: authenticators, claims, data or information, identifiers, presence, relationship representations and reputation. It may have any or many natures (singular, multiple, same, different, fixed, flexible, authentic, fictitious, assumed, assigned, fragmented, cohesive, public, private, anonymous, pseudonymous, temporary, permanent, visible or invisible) which add to its complexity. Given all this, digital identity operates primarily in the context of individuals and shares a profound yet subjective relationship with them.

3. Local Difference: Framing the local context of digital identity

> because it is within cultures that we decide what is valuable and what is not.
> *-Enrico Coiera*[279]

3.1. Introduction

Local difference is an important influence on digital identity, its experience, use and regulation. However, the place of local difference[280] thus far has been ignored in the international digital identity regulatory discourse. This chapter shows how local difference is evident and the critical part it plays in the context of the UK and India.

What is local difference? Difference manifests in the non-equality or the non-conformity of two elements or objects to one another. Local difference, here, refers to the factors that represent a variance between two compared entities. There may be elements or factors in one jurisdiction that cause digital identity to be either experienced or regulated differently as compared to another jurisdiction.[281] Thus, while the same digital identity might subsist in one or more jurisdiction, it is subject to dissimilar experiences according to local conditions.[282]

---

[279] Enrico Coiera, 'The Impact of Culture on Technology: How Do We Create a Clinical Culture of Innovation?' Editorial, (1999) 171 MJA, 508-509

[280] The significance of local difference resonates in: M Castells, JL Qiu, M Fernández-Ardèvol & A Sey, *Mobile Communication and Society: A Global Perspective* (MIT Press, Cambridge 2007); Simon Rogerson, 'The Virtual World: A Tension between Global Reach and Local Sensitivity,' (2004) 2 (11/2004) Intl J of Information Ethics, 1-7; David Hume, *A Treatise of Human Nature 1739* (OUP, Oxford 1978); David Lewis, *Convention: A Philosophical Study* (HUP, MA 1969); Edna Ullmann-Margalit, *The Emergence of Norms* (OUP, Oxford 1977); SJ Simon, 'The Impact of Culture and Gender on Websites: An Empirical Study,' (2000) 32 (1) SIGMIS Database, 18-37; G8, *Digital Opportunities for All: Meeting the Challenge: Report of the Digital Opportunity Task Force (DOT Force) Including a Proposal for a Genoa Plan of Action*, May 2001, <http://www.dotforce.org/reports/>; AA Erumban, SB Jong, 'Cross-country Differences in ICT Adoption: A Consequence of Culture?' (2006) 41 J World Bus, 302–314. Near similar studies were conducted by EM Meijer and R Ling, 'The Adoption and Use of ICT Services in Europe: Potential Acceptance of Mobile Broadband Services,' EURESCOM P903 (2006), <www.eurescom.de/~ftproot/web-deliverables/public/P900-series/P903/ICT_use_ ante.pdf>; SM Lee and SJ Peterson, 'Culture, Entrepreneurial Orientation, and Global Competitiveness,' (2000) 35 J World Bus, 401-416; Y Everdingen and E Waarts, 'The Effect of National Culture on the Adoption of Innovations,' (2004) 14 (3) Marketing Letters, 217–232

[281] In line with De Cruz's reasoning that "norms and patterns of behaviour which one society may deem natural and legal may be characterised as reprehensible and unacceptable in another." Peter De Cruz, *Comparative Law in a Changing World* (Cavendish Publishing, London 1999), 17

[282] This resonates in Legrand's comments on the subject that "there exists a socio-cultural dimension which, although it is largely concealed, remains inherent to rules. Legrand (1996) **n45**

In the instant case, local difference is represented by the factors affecting digital identity that distinguish the UK from India. These factors peculiarly influence and affect its nature, its relationship with the individual, its management and regulation and are examined below.

3.2. Key points of difference

Our research has identified two key areas of difference relevant to digital identity between the UK and India: state of digital technology and the influence of culture. The state of digital technology is explored in relation to operating conditions, penetration, access and use of digital technologies. The influence of culture (attitudes, social values, norms and practices) is explored in relation to important digital identity concepts like privacy, information sharing, communal use of personal information, authentication and verification, openness and transparency and anonymity and pseudonymity.

3.2.1. State of digital technology

The UK is a highly advanced digital country.[283] India, on the contrary, is a digitally advancing country.

The Digital Britain Report 2009 highlights the place of digital technology in the UK.[284] It states,

> Digital technology - and particularly the Internet - is the common backbone for numerous services and devices that most people now take for granted, including MP3 players, web-enabled mobile phones, online gaming, social networking, multi-channel television, digital radio and podcasts. But it is much more than that. Digital technology is no longer simply desirable. It is

[283] See OECD, *OECD Reviews of Regulatory Reform, United Kingdom: Challenges at the Cutting Edge* (OECD, France 2002), 39-40 (categorised as Europe's Internet leader); Nicoletta Corrocher, 'The Internet Services Industry: Country Specific Trends in the UK, Italy and Sweden,' in Charles Edquist (ed), *The Internet and Mobile Telecommunications System of Innovation: Developments in Equipment, Access and Content* (Edward Elgar Publishing, Cheltenham 2003), 210-235, 215; HM Government, *A Better Deal for Consumers: Delivering Real Help Now and Change for the Future*, (OPSI, Surrey 2009), 50 (European leader in Internet shopping); BBC News, 'UK Consumers Enjoy 'Advanced' Digital Communications' (17 December 2009) <http://news.bbc.co.uk/1/hi/8417521.stm>

[284] Department for Culture, Media and Sport and Department for Business, Innovation and Skills, 'Digital Britain,' Final Report, Presented to Parliament by the Secretary of State for Culture, Media and Sport and the Minister for Communications, Technology and Broadcasting (June 2009)

> rapidly becoming an essential facility for citizens and consumers in a modern society.[285]

Digital technology is a basic necessity and has permeated every aspect of life, characterised by pervasiveness and omnipresence.

On the other hand, the situation in India is very contrastive. Digital technologies, though advancing rapidly, have not had a similar impact.[286] This is evident in the following observations:

> India's digital consumption marketplace has clear divisions among urban-rural, rich-poor, and old-young lines. Online content is accessible predominantly to India's young, wealthy and urban populations…India has the highest PC costs and the lowest PC availability[287]…Internet cafes are major venues for Internet access…Mobile Internet has grown faster than fixed-line broadband…[288]

Thus, on one hand, we have a jurisdiction where digital technology is an essential and basic part of life - the UK – and where digital identity is thus fairly well established. On the other, we have India, where digital technology, though progressing at a rapid rate, is still unevenly distributed, affecting the nature of digital identity.

3.2.1.1.Operating Conditions

Digital technologies do not operate in vacuum and they are affected in their development and expansion by local conditions like the nature of society, economy and culture. In Europe and the UK, the nature of society, economy and culture boosts the development and progress of digital technologies.[289] Yet, though India is a hub of

---

[285] Supported by research from the Communications Consumer Panel which found that 70% of people in the UK thought that home broadband was essential.
[286] S Borbora and MK Dutta, 'ICT in Regional Development,' in S Marshall, W Taylor, X Huo Yu (eds), *Encyclopedia of Developing Regional Communities with Information and Communication Technology* (Idea Group, UK 2006), 387-392, 387; UNCTAD, *Information Economy Report 2007-2008* (UN, Geneva 2007), Chapter 2
[287] As compared to Brazil, Russia, China and Indonesia.
[288] Marcos Aguiar and ors, 'The Internet's New Billion: Digital Consumers in Brazil, Russia, India, China and Indonesia,' (September 2010) <http://www.bcg.com/documents/file58645.pdf>
[289] EC, *The Economy of Culture in Europe*, Study Prepared by the European Commission (October 2006), 32; José Manuel Barroso, 'Europe: Art or Science,' Speech, Delft University of Technology, (13 January 2006)

digital technologies, the development and progress of these in India is often hindered by the nature of its society, economy and culture.[290]

The UK is amongst the top digital economies. This is supported by the Digital Economy Rankings 2010[291] aimed at assessing "the quality of a country's ICT infrastructure and the ability of its consumers, businesses and governments to use ICT to their benefit." The UK ranked 14th, while India came 58th. The categories on which countries were judged were: connectivity and technology infrastructure,[292] business environment,[293] social and cultural environment,[294] legal environment,[295] government policy and vision[296] and consumer and business adoption.[297] Here is how the two countries scored:

	Overall Score	Connectivity	Business environment	Social and cultural environment	Legal environment	Government policy and vision	Consumer and business adoption
Category Weight		**20%**	**15%**	**15%**	**10%**	**15%**	**25%**
UK	7.89	7.65	7.40	7.73	8.10	8.55	8.00
India	4.11	2.15	6.27	4.67	5.60	5.10	2.88

Fig 3: Economist Intelligence Unit Digital Economy Rankings 2010

[290] Extensively covered in RK Bagga, K Keniston and RR Mathur, *The State, IT and Development* (Sage, New Delhi 2005).
[291] Economist Intelligence Unit, 'Digital Economy Rankings 2010: Beyond E-readiness,' White Paper, 2010 <http://graphics.eiu.com/upload/EIU_Digital_economy_rankings_2010_FINAL_WEB.pdf>
[292] This category measures the extent and ability of individual and business access to the Internet and mobile networks.
[293] Covers strength of the economy, political stability, taxation, competition policy, the labour market, and openness to trade and investment.
[294] Covers educational levels (measured by school life expectancy, gross enrolment in education and enrolment in tertiary education); Internet literacy; degree of entrepreneurship; technical skills of workforce; degree of innovation (measured by the generation of patents and trademarks, as well as R&D spending).
[295] Reflecting legal frameworks with a direct impact on the use of digital technology and measures the effectiveness of traditional legal framework, Internet laws, censorship levels, ease of registering a new business and electronic ID.
[296] Covers government spend on ICT as a proportion of GDP, digital development strategy, e-government strategy, online procurement, availability of online public services for citizens and businesses and e-participation.
[297] Includes consumer spending on ICT per head, level of e-business development, use of Internet by consumers, assessing both the range of Internet features used by individuals and their online purchasing activity, use of online public services by citizens and businesses.

From the data, vast differences are apparent between the two countries in regards to the conditions under which digital identity technologies operate. The UK performs far better than India – it has superior connectivity, a marginally finer business environment and a highly conducive social, cultural and legal environment, as compared to India. It also has a government policy and vision that is more conducive to the growth of digital technologies and a high level of business and consumer adoption of digital technologies.

3.2.1.2.Penetration of Digital Technologies

According to data from the ITU,[298] in 2006, for every 100 people in the UK, there were 80 personal computers;[299] while in India there were only 2.79 personal computers for every hundred people.[300] Variance shows in respect of the number of Internet users too. In 2008, UK had 76 Internet users per 100 people while India had only 4.54.[301]

Though the penetration of digital technologies, particularly mobile phones has substantially increased and is constantly improving in India, it leaves much to be desired in terms of universality. The penetration of digital technologies is highly uneven,[302] and on international comparison, abysmal.[303] Narayan highlights this in terms of what he calls the "yawning gap between individuals, households, businesses and geographic areas at different socio-economic levels."[304]

---

[298] See World Development Indicators, <http://data.worldbank.org/indicator/IT.CMP.PCMP.P2>
[299] Defined as "self-contained computers designed to be used by a single individual."
[300] Reported to have increased to 3.29 in 2007.
[301] See World Development Indicators, <http://data.worldbank.org/indicator/IT.CMP.PCMP.P2> and <http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/latest?display=default>
[302] O Manzar and SS Kazi, '.in India,' in S Akhtar and P Arinto (eds), *Digital Review of Asia Pacific 2009-2010* (Sage, New Delhi 2009), 192-200, 192
[303] Borbora (2006) **n286**, 387-392, 387
[304] Jayaprakash Narayan, 'Governance: Virtual to Real,' in RK Bagga, K Keniston and RR Mathur (eds), *The State, IT and Development* (Sage, New Delhi 2005), 43-67, 48

3.2.1.3.Access to digital technologies

A denial or lack of access to digital technologies affects the enjoyment of digital identity.[305] Access to digital technologies is also at enhanced levels in the UK as compared to India. This is particularly evident in the widespread access to and use of the Internet[306] and mobile services[307] (two key digital identity platforms) which borders on the near universal, shaped by policy that promotes this.[308] Access to digital technologies in India is poor. Even in urban areas in India where digital technology generally flourishes, it only works to serve the needs of a "fraction of the population."[309]

Exposure and access to digital technologies in India is hampered by a number of factors. First, the vast majority of India's population lives in rural settlements,[310] where digital infrastructure has not effectively permeated. Computer and Internet penetration is low (though several initiatives have been launched to correct this).[311] This restricts access of individuals to these technologies and affects the mediation of their identity. Additionally, other socio-economic conditions (like wealth, education, gender,[312] caste or class based discrimination in access to and use of technologies)[313] contribute to furthering the access divide. [314]

---

[305] C Murroni and N Irvine, *Access Matters* (IPPR, London 1998)
[306] Ronald Deibert, JG Palfrey, R Rohozinski, J Zittrain (eds), *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (MIT Press, Cambridge 2010), 358
[307] Deibert (2010) **n306**, 76
[308] See Digital Britain (2009) **n284**; Allen Booz and Hamilton, 'Achieving Universal Access,' A Report for the Prime Minister's Policy Unit (2000); Tony Blair's full speech, *The Guardian* (7 March 2000) <http://www.guardian.co.uk/technology/2000/mar/07/internet.uknews>
[309] Jonathan Fildes, 'India's Vision for a Digital Billion,' *BBC News* (6 February 2007) <http://news.bbc.co.uk/1/hi/technology/6322027.stm>
[310] Mark Warschauer, *Technology and Social Inclusion:Rethinking the Digital Divide* (MIT Press, 2004), 61
[311] See P Gupta and RK Bagga (eds), *Compendium of E-Governance Initiatives in India* (Universities Press, India 2008)
[312] Sarita Seshagiri, Sagar Aman and Dhaval Joshi, 'Connecting the "Bottom of the Pyramid": An Exploratory Case Study of India's Rural Communication Environment,' in *Proceedings of the 16th International Conference on the World Wide Web* (ACM Press, NY 2007), 855-862. The study shows men enjoy a powerful status in a village as decision makers and controllers of digital technologies like mobile phones. See also Rekha Pande, 'Digital Bridge or Digital Divide: Assessing Gender Equations and the Indian Experience in Information and Communication Technologies,' Paper Presented at the Annual Meeting of the International Studies Association, Montreal, Canada (17 March 2004).
[313] Robert Jensen, 'The Digital Provide: Information (Technology), Market Performance and Welfare in the South Indian Fisheries Sector,' (2007) 122 (3) Q J Econ, 879-924
[314] For an in-depth discussion of connective issues see Kenneth Keniston & Deepak Kumar (eds), *IT Experience in India: Bridging the Digital Divide* (Sage, India 2004)

3.2.1.4.Use of digital technologies

While there are general parallels in the use of digital technologies across the world, and the UK and India, there are also vast differences in use of these technologies. This is examined below in the context of computers, the Internet and mobile phones. A single individual in the UK often owns a multiplicity of digital devices; and these devices, like computers, laptops, PDA's and mobile phones[315] are perceived, characterised and used as personal objects. Conditions like the wide, easy availability and affordability of these devices in the UK facilitates and promotes this culture and practice. On the other hand, in India, computers, laptops and even mobile phones are not as widely or easily available, affordable or used as 'personal' objects. This makes them more exposed to being shared[316] (though this is not the only motivation behind shared use of digital technologies). Three studies support this contention.

The first is Miller's study on computer and Internet usage in a village in South India.[317] The study highlights how several residents of an area visit an electrician's home and use his computer to send emails, surf the web, download material and entertain themselves. The electrician functions as a digital service provider who shares his digital resources with his fellow villagers who are not as fortunate in having access to the digital resources available to him. The computer functions as a communal resource that enables many individuals to use digital technology and express their digital identities.

The second study is that of Seshagiri, Aman and Joshi, conducted in a village in the Chamrajanagar district of Karnataka, India.[318] The study aimed to "understand the rural communication environment and villagers' communication preferences" in relation to mobile phones. It found that where mobiles and landlines were limited in

---

[315] Even if these technologies are shared, this would be very limited in comparison to the practice in India. The mobile phone is particular is viewed as a highly personal means of private communication between individuals. See Maren Hartmann, P Rössler and JR Höflich, *After the Mobile Phone? Social Changes and the Development of Mobile Communication* (Frank and Timme, Berlin 2008), 35

[316] A Pentland, R Fletcher and A Hasson, 'Dak Net: Rethinking Connectivity in Developing Nations,' IEEE Computer Society, (January 2004), 78 – 83; Rekha Jain, 'The Telecoms Sector: India Infrastructure Report 2001,' <http://www.iitk.ac.in/3inetwork/html/reports/IIR2001/iir8.pdf>

[317] Eric Miller, 'Wireless Internet Access in Rural South India' (December 2000) <http://ccat.sas.upenn.edu/~emiller/report.html>

[318] Seshagiri (2007) **n312,** 855-862

availability due to their costs, they became shared devices. The sharing occurred between family members, close friends and even acquaintances.[319]

The third study, conducted by Chittamuru,[320] was a qualitative study on the use of mobile phones by children in the villages of Kanaar and Gulab Kheda, in Uttar Pradesh, India. A number of key observations were made,[321] one of which was in respect of the shared use of digital technologies. A mobile given for the exclusive use of a female child was taken away by her brother and used by him for his own ends (he even put his own name on it). Her phone functioned as a communal communication instrument."[322] In cases where the female child objected to such use, she was asked by her family to defer to her brother's wishes. Here, a social norm affects the female child's ability to effectively experience and enjoy her digital identity. That the sharing of digital identity devices like mobile phones is common in India[323] and affected by social norms is also supported by Konkka's research on mobile usability in Mumbai.[324] This study distinguishes Indian mobile phone use from Western phone use and outlines how mobile use in India is commonly characterised by the sharing of devices and calls.

Thus, there is evidence of local difference in the experience and use of digital identity technologies between the UK and India. These are crucial to and have far reaching implications for digital identity, its management and regulation.

---

[319] It was reported that there were only 7 mobile phones in the village with 160 households.
[320] Deepti Chittamuru, 'Millee: Social Dynamics Of Mobile Phone Use By Children In Rural India,' Capstone Project Paper (Spring 2009), <http://www.ischool.berkeley.edu/files/student_projects/MILLEE-_SOCIAL_DYNAMICS_OF_MOBILE_PHONE_USE.pdf>
[321] For full details, see study.
[322] Manuel Castells, M Fernandez-Ardevol, JL Qiu and A Sey, *Mobile Communication and Society: A Global Perspective* (MIT Press, Cambridge 2007), 64
[323] See AL Chavan, 'A Dramatic Day in the Life of a Shared Indian Mobile Phone,' in NM Aykin (ed), *Usability and Internationalization: HCI and Culture,* Lecture Notes in Computer Science, 4559/2007, (Springer 2007, New York), 19-26
[324] K Konkka, 'Indian Needs: Cultural End-user Research in Mombai,' in C Lindhom, T Keinonen, & H Kiljander, (eds), *Mobile Usability: How Nokia Changed the Face of the Mobile Phone* (McGraw-Hill, New York 2003), 97-112

3.2.2. The influence of culture: Attitudes, Social Values, Norms and Practices

The UK and India are culturally distinct when compared to one another. Though both have sub-cultures (for instance, UK has English, Welsh, Scottish and Irish, and India has a vast diversity manifest in varied customs, traditions, social practices, languages etc), they each have overall core national cultures[325] that set them apart from each other. This is proved extensively in the studies of Hofstede[326] and Trompenaars and Hampden Turner.[327]

Hofstede[328] classified national cultures according to four dimensions: power distance,[329] uncertainty avoidance,[330] individualism[331] and masculinity.[332] Hofstede's study[333] revealed that India has high levels of power distance (indicative of high levels of inequality of power and wealth inequalities), very low levels of uncertainty avoidance, low levels of individualism and high levels of masculinity. Comparatively, the UK was found to have low power distance, nearly equal levels of uncertainty avoidance, extremely high levels of individualism and low levels of

---

[325] Jawaharlal Nehru, *The Discovery of India* (Signet Press, Calcutta 1946); R Ramanathan, 'Globalisation, Values and Democracy,' (February 2004) <http://www.indiatogether.org/2004/feb/opi-values.htm>

[326] Hofstede (1980) **n28**; Hofstede (1994) **n28,** 13-15

[327] Hampden-Turner (1997) **n28**

[328] Hofstede (1980) **n28**

[329] Denoting "the extent to which the less powerful members of organizations and institutions (like the family) accept and expect that power is distributed unequally."

[330] Denoting "society's tolerance for uncertainty and ambiguity; it ultimately refers to man's search for Truth."

[331] Characterised by loose individual ties in society.

[332] Meaning gender based role distribution.

[333] Hofstede has his critics. See L Goodstein, 'Do American Theories Apply Abroad: American Business Values and Cultural Imperialism,' Commentary, (Summer1981), Organizational Dynamics, 49-54; J Hunt, 'Do American Theories Apply Abroad: Applying American Behavioural Science, Some Cross Cultural Problems,' (Summer 1981) *Organizational Dynamics*, 55-62; K Roberts and N Boyacigiller, 'Cross-national Organizational Research: The Grasp of the Blind Men,' (1984) 6 Research in Organizational Behaviour, 423-475; DR Fernandez, DS Carlson, LP Stepina, and JD Nicholson, 'Hofstede's Country Classification 25 Years Later,' (1997) 137 (1) *The Journal of Social Psychology,* 43-54. Yet, his findings are still internationally relevant, accepted and used in international multi-disciplinary research. Schuman in particular cites several reasons for the wide acceptance of his work: profound empirical foundation, theoretical foundation and external validity, its external validity in different disciplines. JH Schumann, *The Impact of Culture on Relationship Marketing in International Services:A Target Group-Specific Analysis in the Context of Banking Services* (Deustche Nationalbibliothek, Munchen 2009), 58; Wolfgang Messner, A Hendel, F Thun, 'Rightshore,' in Wolfgang Messner (ed), *Intercultural Aspects of Project Management in India* (Springer, Berlin 2008), 101-120; Aaron Marcus, 'Global and Intercultural User Interface Design,' in JA Jacko and A Sears (eds), *The Human Computer Interaction Handbook* (LEA Publishers, NJ 2003), 441-463

masculinity. The UK is, thus, a society in which "ties between individuals are loose."[334] India on the other hand, is a society in which the ties between individuals are strong, cohesive, integrative and lifelong.[335]

Cultural differences between the UK and India were also identified by Trompenaars and Hamden Turner[336] in relation to various dimensions: universalism and particularism (rules and relationships), communitarianism and individualism, affectivity and neutrality (displaying and concealing emotions), specificity and diffusion (connected to Hall's low and high context), [337] achievement and ascription (what one does and who one is), inner and outer direction and sequential and synchronic time. Their study demonstrated that the UK is a highly universalist and individualist national culture – one where there is a greater tendency to focus on rules and perceive the group interests largely in terms of achieving their own individual interests. India was found to be a particularist and communitarian culture which meant a tendency to focus more on relationships and view individual interests as largely allied or dependent on group interests.

In addition to this, other research argues and demonstrates that there is significant cultural difference between the UK and India. For instance, Dumont,[338] Cohn,[339] Triandis [340] and Kakar.[341] Despite, all this, this chapter does not take these for a given. In keeping with Capurro's exhortation, to not just

> … compare similar or dissimilar concepts by juxtaposing them, or to look for a conceptual or even moral consensus – but to become aware of our mutual

[334] Hofstede (1994) **n28,** 51
[335] Hofstede (1994) **n28**, 51
[336] Hampden-Turner (1997) **n28**
[337] ET Hall, *Beyond Culture* (Bantam Doubleday, NY 1997)
[338] See L Dumont, *Homo Hierarchicus*: *The Caste System and its Implications* (U Chicago Press, US 1970), 8-9
[339] BS Cohn, 'The Census, Social Structure and Objectification in South Asia,' in BS Cohn, *An Anthropologist Among Historians and Other Essays* (OUP, New Delhi 1987), 224-254.
[340] HC Triandis, R Bontempo, MJ Villareal, M Asai, N Lucca, 'Individualism and Collectivism: Cross-cultural Perspectives on Self-ingroup Relationships,' (1988) 54 (2) Journal of Personality and Social Psychology, 323-338
[341] S Kakar, *The Inner World: A Psycho-Analytic Study of Childhood and Society in India* (OUP, Delhi 1981), 37; BK Ramanujam, 'Toward Maturity: Problems of Identity Seen in the Indian Clinical Setting,' in S Kakar (ed.) *Identity and Adulthood* (OUP, 1979), 37-55, 54

> biases on the basis of a nuanced understanding of similarities and dissimilarities beyond the simple dichotomy between ''East'' and ''West,''[342]

it examines for itself how local difference manifests in the cultural context in principal digital identity contexts like privacy, information sharing, communal use of personal information, authentication and verification, openness and transparency and anonymity and pseudonymity.

3.2.2.1.Privacy: Expectations, architecture and norms

Privacy is as much a cultural concept (it is generally recognised as having western roots) as it is a legal one.[343] It is interpreted differently in different countries and assumes different connotations.[344] For instance, there are fundamental differences in the philosophy of privacy of the United States and the European Union.[345] Whitman cites as an example the public disclosures in the Monica Lewinsky scandal that confounded European privacy sensibilities.[346] Even within these major blocks there are internal differences.[347] Privacy for individuals in the UK connotes something different from what it would for individuals in India. [348] It is stated that the British (and particularly the English), "are very reserved, private people for the most part."[349] The converse is stated of Indians.[350] Even the conception of what is private and what constitutes private space has much conceptual and practical distinction in the two countries.

---

[342] R Capurro, 'Privacy: An Intercultural Perspective,' (2005) 7 Ethics and Information Technology, 37-47.
[343] David Lyon, *Surveillance Studies: An Overview* (Polity Press, US 2007)
[344] RC Post, 'Three Concepts of Privacy' (2001) 89 Geo. LJ, 2087
[345] D Heisenberg and M-H Fandel, 'Projecting EU Regimes Abroad: The EU Data Protection Directive as Global Standard,' Paper presented at the Annual Meeting of the American Political Science Association, Boston, Massachusetts (28 August 2002) <http://www.allacademic.com/meta/p65517_index.html>
[346] See JQ Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty," (2004) 113 Yale Law Journal 1151, citing 'Le Recours à l'Intimité est de Règle aux Etats-Unis, *Le Monde* (22 Avril 2002); Jacques Lassaussois, 'Procès Clinton : Où va la Justice Américaine? *Gazette du Palais,* (18-19 March 1998)
[347] Reiterated in JA Cannataci, 'Privacy, Technology Law and Religions Across Cultures,' 2009 (1) JILT, <http://go.warwick.ac.uk/jilt/2009_1/cannataci>
[348] This is substantiated by Westin's comments in regard to the differential nature of national cultures of privacy. He stated that England was characterised by "a greater personal reserve between Englishmen, high personal privacy in home and private associations, and a faith in government that bestows major areas of privacy for government operations. AF Westin, *Privacy and Freedom* (Atheneum Press, NY 1967), 26-27
[349] Kevin Myers, 'English Character and Identity,' in Gary Taylor and Steve Spencer (eds), *Social Identities: Multidisciplinary Approaches* (Routledge, Oxon 2004), 129-144, 131; J Oakland, *British Civilization: An Introduction,* (Routledge, London 1998), 66; AM Sabath, *International Business Etiquette: Europe* (Career Press, USA 2005), 63
[350] Wolfgang Messner, *Working with India* (Springer-Verlag, Berlin 2008), 118; Craig Storti, *Bridging the Communication Gap When Working with Indians* (Intercultural Press, USA 2007), 20

Privacy differences in the two countries are comparatively analysed next in respect of expectations, living architecture and norms. This is particularly relevant to holistically understand local difference as recommended by the report prepared for the Commission of the European Communities, Directorate-General for Justice, Freedom and Security.[351]

3.2.2.1.1. Expectations

Privacy differs in the expectations people of different countries have of it.[352] This is confirmed by Nouwt, de Vries and Loermans,[353] and is not unusual given the subjective nature of privacy. In this light, privacy expectations in the UK would demonstrate variance from privacy expectations in the India.

While there is no empirical research comparing the UK and India in respect of privacy expectations, there is research showing that Indian privacy perceptions differ from those in the digitally advanced West. Kumaraguru, Cranor and Newton's interview study on privacy perceptions investigated the differences in privacy perceptions between the US and India.[354] The Indian respondents in the study visualised privacy primarily in terms of personal space while the US respondents visualised privacy more in terms of their personal information. 61 percent of the US respondents made a connection between privacy and personal information control while only 14 percent of the Indian respondents made a similar connection. 48 per cent of the Indian respondents connected privacy to their physical, home and living space. Correspondingly, only 18 percent of US respondents related privacy to these. The study thus affirms that privacy expectations between countries vary.

---

[351] CRID (University of Namur), First Analysis of the Personal Data protection Law in India, Report delivered in the Framework of Contract JLS/C4/2005/15 between CRID and the Directorate General Justice, Freedom and Security <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf>

[352] A point also made by DJ Solove, *Understanding Privacy* (HUP, Cambridge 2008), 75; Sandra S Petronio, *Boundaries of Privacy: Dialectics of Disclosure* (SUNY Press: Albany 2002), 223

[353] Sjaak Nouwt, BR de Vries and R Loermans, 'Analysis of the Country Reports,' in Sjaak Nouwt, BR de Vries & C Prins (eds), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (TMC Asser Press, The Hague 2005), 352

[354] P Kumaraguru, L Cranor and E Newton, 'Privacy Perceptions in India and the United States: An Interview Study,' 33rd Research Conference on Communication, Information and Internet Policy, The National Center for Technology and Law, George Mason University School of Law, USA, (23 -25 September 2005)

3.2.2.1.2. Architecture

Life in general constructs the norms of privacy. The life environment of an individual has significant impact on privacy, and how it manifests itself.

Though the UK is one of the most densely populated countries in Europe, in comparison to India, which at the time of writing is the second largest populated country in the world, physical living conditions in the UK are highly advantageous to privacy. On average, people in the UK occupy 44 square metres of dwelling space,[355] with 2.3 persons per dwelling.[356] There are a high number of single person households,[357] with only 7 percent of households in the UK comprising of more than four persons.[358] Individuals live in conditions that favour the exercise of personal privacy as against other individuals or the rest of the world by default.

On the other hand, living conditions in India on the whole are unfavourable to privacy, particularly personal privacy.[359] In 2008, the NSSO survey reported that around 32 percent of houses in urban areas were 258 square feet or less in area, with an average household size of 4.3 persons. 39 percent of rural houses were 312 square feet or under with an average household size 4.8 persons. Individuals live in cramped quarters which they share with many others and this affects how they live, sleep, eat, and conduct other social activities.[360]

It is not just household space that makes privacy difficult to exercise. In villages, houses are often built in close proximity, with materials like mud or thatch that do not afford effective separation from the community. This is in vast contrast to the

---

[355] For owner occupied homes, 46m^2 and social housing, 36m^2. Office of the Deputy Prime Minister, 'English House Condition Survey, 2001: Building the Picture,' (ODPM, London 2003).
[356] See 2001 Census.
[357] Office for National Statistics, *Social Trends 34: National Statistics* (The Stationery Office, London 2004)
[358] Katie Williams, 'Space Per Person in the UK: A Review of Densities, Trends, Experiences and Optimum Levels,' Review, (2009), 26S Land Use Policy, S83–S92, S85
[359] CAK Yesudian, *Health Services Utilisation in Urban India: A Study* (Mittal Publications, Delhi 1988), 94; M Soundarapandian, *Literacy Campaign in India* (Discovery Publications, New Delhi 2000), 119; Kathleen Gough, *Rural Society in South East India* (CUP, UK 1981), 159, 282; AC Mayer, *Caste and Kinship in Central India* (University of California Press, Berkeley 1960), 16
[360] See Atul Thakur, '33% of Indians Live in Less Space than US Prisoners,' *The Economic Times*, (25 November 2008) <http://economictimes.indiatimes.com/News/PoliticsNation/33-of-Indians-live-in-less-space-than-US-prisoners/articleshow/3754519.cms>

UK, and means that individuals in India do not generally have an established privilege of exercising personal privacy against other individuals or the rest of the world by default.

Despite nuclear families becoming fashionable in India, joint families are widespread.[361] In joint families, "members of a unilineal descent group (a group in which descent through either the female or the male line is emphasized) live together with their spouses and offspring in one homestead and under the authority of one of the members."[362] Even outwith the joint family system, a large number of people live in crowded family clusters. Particularly in rural areas large families are prevalent. These offer little to encourage privacy, as expressed in Adiga's *White Tiger*: "I shake my brother Kishan's legs off my tummy, move my cousin Pappu's palm out of my hair, and extricate myself from the sleepers."[363]

Now place the use of digital identity technologies in the context of these architectures. Let's take the case of a home computer, shared by many individuals living under the same roof. The home computer is accessed in full public view of one's family, perhaps with someone looking constantly over one's shoulder. The computer might even be accessed by two or more members of the family at the same time, [364] as depicted below:

Fig 4: Shared computer access[365]

[361] Raghuvir Sinha, *Dynamics of Change in the Modern Hindu Family* (AKMC, New Delhi 1993), 22
[362] Encyclopædia Britannica, 'Joint family,' <http://www.britannica.com/EBchecked/topic/305637/joint-family>
[363] A Adiga, *The White Tiger* (Atlantic Books, London 2008), 21
[364] Ann Hsieh, Todd Hausman and Nerija Titus, 'Influencers and Their Barriers to Technology,' in *Proceedings of the 17th International Conference on World Wide Web* (WWW '08) (ACM, NY 2008), 1103-1104
[365] Image courtesy: Outlook India, <http://www.outlookindia.com/images/computer_20080505.jpg>

Thus, the architectures of living in India do not augur well for the privacy of digital identity, as compared to the UK.

3.2.2.1.3. Norms

Privacy, though expressed restrictively, as a norm, is not entirely absent in India. It is a well established principle in relation to the human body and certain acts in relation to it.

The human body (particularly the female) is considered sacred and worthy of privacy.[366] Violation of bodily privacy particularly in respect of the intimate zones is frowned upon and draws social censure. For instance, as demonstrated by the Soman-Sapre incident. Models Madhu Sapre and Milind Soman posed nude in an advertisement for Tuff shoes wearing only a python between them. Extensive protests followed and charges were levelled against them for obscenity and indecent representation of women.[367] The exposure of the intimate parts of the human body was considered a violation of the privacy interest in the body and contrary to social norms.

Privacy is also established in terms of protecting the honour and dignity of women.[368] Many women in India (particularly Hindu and Muslim) wear a veil to shield themselves from the public gaze, particularly outside their intimate family or kinship circles. Women are careful about exposing cleavage and upper legs.[369] Women wear *saris* (ankle length) with its *pallu* (part that drapes over shoulders and can be used to cover head), *salwar-kameez's* with a *dupatta* that covers the bosom and head, *lehngas* in Rajasthan (again ankle length) with an *odhni* (long scarf). Clothing, here, functions as a privacy norm enabler. In cases where this norm is

[366] There is some religious basis for this. Hinduism, for instance, reveres bodily sanctity and privacy. This is evident in the account of Goddess Parvathi taking active steps to protect her bodily privacy in *Shiva Purana, Rudra* 13.15-37, 17.3-59. See Carl Olson, *The Many Colours of Hinduism* (Rutgers University Press, NJ 2007), 225

[367] Nitasha Natu, 'Tuff Shoes Case: Madhu, Milind Plead Not Guilty,' *Times of India* (29 October 2004) <http://timesofindia.indiatimes.com/articleshow/903786.cms>

[368] This cultural concern is also reflected in law. See **Chs 5 (5.2.2.1.2) & 6 (6.3.1.2)**

[369] There are exceptions to this rule, particularly in urban areas where Western fashion has made an impact and attitudes are more liberal. Other exceptions can be found in tribal areas where social norms permit such trends.

disregarded, consequences result (e.g. harassment of women who wear skimpy clothing).[370]

Another aspect where privacy norms strongly apply in India, are public displays of affection between the sexes.[371] Such displays are considered part of the private realm.[372] For instance, kissing in public (between a male and female) is considered alien to culture, "western" and "against *sanskar*."[373] When actor Richard Gere publicly kissed actress Shilpa Shetty at an AIDS awareness rally, it resulted in public outrage and criminal complaints being filed against him.[374] Though this practice is gaining acceptance, it remains largely restricted by social censure,[375] as evident in the following statement:

> In our customs, we are an open society and holding hands is no problem, but kissing in public we do not entertain at all.[376]

This is despite the Supreme Court of India[377] and other courts[378] ruling that public kissing by a married couple does not amount to an obscenity. Even in India's popular movie culture, kissing scenes were prohibited from depiction until around 2000- based on unwritten rules of traditional culture,[379] a world where kissing, "belongs to the realm of the private."[380]

---

[370] Joe Bindloss, Lindsay Brown, Mark Elliott and Paul Harding *North East India* (Lonely Planet, Victoria 2007), 317; Sarina Singh, *South India* (Lonely Planet, Victoria 2007), 490
[371] David M Kennedy Center for International Studies, *Culturgrams: Middle East, Asia, Africa, and Pacific Areas* (The Center, 1988)
[372] Rujul Pathak, 'No Public Display of Affection Please, We Are Indian!' *Times of India* (5 June 2003) <http://timesofindia.indiatimes.com/Ahmedabad-Events/No-public-display-of-affection-please-we-are-Indian/articleshow/45961507.cms#ixzz0zhQ209g5>
[373] *Sanskar* here refers to morality. See CA Joseph and AP Kavoori, 'Mediated Resistance: Tourism and the Host Community,' (2001) 28 (4) Annals of Tourism Research, 998-1009
[374] The Associated Press, 'Gere Kiss Leads to Legal Complaints in India,' (18 May 2007) <http://www.usatoday.com/life/people/2007-04-16-gere-kiss_N.htm>
[375] The Delhi High Court recognised this in *Virender v State of NCT of Delhi* Crl.A.No. 121/2008, § 41
[376] Dean Nelson, ''Romantic' Darjeeling Bans Public Displays of Affection,' *Telegraph News* (7 September 2009) <http://www.telegraph.co.uk/news/worldnews/asia/india/6146863/Romantic-Darjeeling-bans-public-displays-of-affection.html>
[377] *Arun Ghosh v State of West Bengal* [1970] 1 SCC 98
[378] *A & B v The State of NTC of Delhi* Crl MC 283/2009
[379] M Madhava Prasad, 'The State and Culture: Hindi Cinema in the Passive Revolution' (PhD dissertation, University of Pittsburgh 1994)
[380] KM Gokulsing and W Dissanayake, *Indian Popular Cinema: A Narrative of Cultural Change* (Trentham Books, England 2004), 81

So, though there are norms of privacy in Indian culture, they are expressed in what might be termed from the Western point of view, a highly conservative conceptualisation of privacy (though the Indian digital identity subject would not see it thus). An Indian digital identity subject would be bound by principle and more likely to protect privacy in the terms of the norms he or she is familiar with (e.g. protection of bodily privacy and female modesty) and not those he or she is unfamiliar with, in particular not as an aggressive assertion of a right towards other community members.

There is strong culture and practice of privacy in the UK. People are generally aware, conscious and act upon their privacy interests. On the other hand, in India there is no parallel awareness, consciousness and action upon similar privacy interests. Privacy has rather a limited connotation here, and this then feeds into how Indian digital identity subjects relate to their digital identity. It might be the reason why the digitally advanced West perceives privacy as a key aspect of digital identity and the why this is not the case in India where digital identity subjects seem relatively lax about the privacy of their digital identity.

The above analysis shows that there are clear differences in privacy expectations, architecture and norms between the UK and India which ultimately feed into an individual's relationship with his digital identity and how digital identity is experienced, used and regulated.

3.2.2.2.Information sharing

Culture also affects attitudes and treatment of personal information.[381] Therefore, attitudes to and the treatment of personal information vary from society to society. Here we take as a given that different cultures conceptualise what constitutes personal information differently.

[381] See DL Stone and EF Stone-Romero, *The Influence of Culture on Human Resource Processes and Management* (Lawrence Erlbaum Associates, Mahwah 2007)

This is highly significant for the study of the legal regulation of digital identity because it then teaches us about why different societies differently relate, deal and regulate such personal information. It also advances our information of how digital identity subjects relate to and deal with their personal information. Let's therefore examine how local difference in culture affects personal information.

In some societies, large amounts of personal information ordinarily reside in the private sphere, unless it is by necessity or consent thrust into the public sphere. Personal information here could refer to name, address and telephone number, sex, age, occupation, salary, nationality, photographs, or records (e.g. medical, financial). There is a general acknowledgement and respect for the privacy of such personal information which is fostered by the manner in which such a society is structured and operates. As a general rule, people are cautious about whether, with who and what personal information (or personal data) is shared.[382] Active steps are generally taken to protect and safeguard it. Society, in its different elements, encourages such a norm through purely social, technical, legal (e.g. privacy and data protection law) or a blend of different measures. The UK is an example of a society where personal information and personal data and is largely resident in the private sphere and is consequently discriminately distributed.[383] Thus personal information and data attains 'gated' or 'walled' dimensions.

On the other hand, there are other societies like India, where by default, and as demonstrated before, large amounts of personal information ordinarily resides in the shared or public sphere,[384] as opposed to being 'walled' or 'gated' within the private sphere. Information or data is generally freely, widely accessible and viewed as part of the collective commons. Individuals in the social and cultural context are not generally viewed as having autonomy over any information or data that relates to,

---

[382] ICM Research, 'Personal Information Survey,' (February 2008) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/icm_research_into_personal_information_feb08.pdf>

[383] There are exceptions to this. Individuals online often demonstrate laxity in this respect, freely sharing and trading personal data.

[384] See Jessica Rewa, 'The True Public Sphere of India: Withstanding the Threats of Globalization and Consumerism,' (2007) <http://drcdev.ohiolink.edu/bitstream/handle/123456789/3631/JessicaRewa2007.pdf?sequence=1>

identifies, authenticates or verifies them. Personal information is not viewed and does not manifest itself as the personal property of an individual, rather more often as a shared communal resource, that only has relevance in this context.

The architecture of life, particularly in villages in India which are close knit communities, facilitates the sharing of personal information. The following quote from R K Narayan's, *The Man Eater of Malgudi* sets the context:

> Our postman, Thanappa, whom we had known as children, old enough to have retired twice over but somehow still in service, was my first visitor for the day… At his favourite corners, he spread out his letters and bags and packets and sat down to a full discussion of family and social matters; he served as a live link between several families, carrying information from house to house...[385]

Villagers often resort to the use of common facilities like the village playing field, pond, grazing grounds, religious places, schools and sheltered spaces under trees to share information of all kinds (including information of highly personal and sensitive nature). Even family courtyards and balconies are spaces that facilitate the casual and routine sharing of personal information.

This trend is reflected in the behaviour of Indian digital identity subjects online, particularly on social networking sites[386] and even other digital information systems. For example, as happened when the VoiKiosk[387] was tested in an agricultural village called Juvvala Palam in South India.[388] Even though personal information and data sharing or social networking was not the primary use of the VoiKiosk, villagers used the VoiKiosk for precisely for these purposes: An eight grade student introduced himself and shared his mobile number. A man uploaded his personal profile so he could find a wife. Both instances demonstrate how open and unperturbed people are about sharing their personal data or information.[389]

---

[385] RK Narayan, *The Man-Eater of Malgudi* (Penguin, England 1983), 158.
[386] P Dixit, 'Social Networkers: A New Generation,' *Hindustan Times* (14 January 2011)
[387] A VoiKiosk is a voice based community information system with a VoiceSite where locally relevant content can be uploaded and accessed by means of a telephone.
[388] SK Agarwal, 'Content Creation and Dissemination by-and-for Users in Rural Areas' (April 2009) <http://www.researchintouse.com/downloads/spokenweb/VoiKiosk_-_ICTD_09_-_April_09.pdf>
[389] *Ibid*

Personal information also has a wider circle of coverage in relation to who is privy to it in India, than in the UK. The dynamic Indian joint family tradition and close knit social structure contributes to this. This is highlighted by Kumaraguru and Cranor, who reveal how the dynamic and Indian joint family tradition and social structure "results in more routine sharing of personal information among a wider group of people" and "information that might typically be disclosed only to one's spouse or parents in the US is more frequently shared among uncles, aunts, and cousins in India."[390]

Even sensitive personal information like medical information is treated differently. In the UK, the privacy of medical information is a given and respected as such; not so in India. For instance, if a person falls sick in India, that fact becomes public information as it gets communicated from family to kin, friends, acquaintances and even the wider community with or without the consent of the concerned individual. Even if one wants to shield this information, it is practically impossible, due to the nature and manner of social relations. In fact, the hiding or shielding of such information could lead to breakdown of social relations (e.g. ties between two families could break where one conceals information from the other). This is symbolic of the collectivist nature of Indian society that places a high premium on sharing personal information within and between groups.

In the UK, according to established social norms, the individual to whom the medical information relates has a choice of disclosing the information, and is aided by social rules that facilitate this. Even where the sharing of information relating to such medical conditions occurs, it is often based upon consent of the individual to whom the information relates.

Let's explore this further in the context of medical data. In the UK, there is a general recognition that a person attending a medical facility has an expectation of privacy in their medical data.[391] The main findings of research conducted by the NHS

[390] Kumaraguru (2005) **n354**
[391] See the DH/IPU/Patient Confidentiality, 'NHS Confidentiality Code of Practice,' (November 2003) § 10,

Information Authority support this contention.[392] People trusted the NHS to protect the privacy of their personal data. They expressed concern about who was entitled to use their data and whether it would be anonymised before further use. They also expressed that any information released beyond the base necessary requirement (release and sharing with GP's, hospital doctors and emergency personnel) should only be on a need-to-know basis.[393]

The current norms in respect of medical data (prompted by need and law of data protection), in the UK favour a "cautious approach towards the use and disclosure of patient data."[394] This is evident in a number of places.

The NHS Confidentiality Code of Practice[395] sets out a confidentiality model to be followed in respect of patients' identifiable information.[396] The Model advocates the following: the protection of a patient's information, ensuring that patients are aware of how their information is used, allowing patients the ability to decide whether their information can be disclosed or used in particular manners, and the need to improve on ways to protect, inform and provide choice.

The General Medical Council (GMC) guidance on Confidentiality[397] is another example. The Guidance, amongst other things, advises personal information may be disclosed only if (a) it is required by law, (b) the patient consents – either implicitly for the sake of their own care or expressly for other purposes and (c) it is justified in

---

<http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4069254.pdf>; B Gross, 'Information Sharing Within and Outwith the NHS,' CSAGS Secretariat, (30 November 2000) § 1 <http://www.csags.scot.nhs.uk/Meeting%20Papers/CSAGS%202000-03.PDF>

[392] NHS Information Authority, The Consumers' Association and Health Which, 'Share with Care: People's Views on Consent and Confidentiality of Patient Information,' Final Report (October 2002) <http://www.connectingforhealth.nhs.uk/resources/archive/share_with_care.pdf>

[393] Ibid, 10

[394] ICO, 'Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998' (May 2002) <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/health_data_-_use_and_disclosure001.pdf>

[395] DH/IPU/Patient Confidentiality (2003) **n391**

[396] This includes: patient's name, address, full post code, date of birth; pictures, photographs, videos, audio-tapes or other images of patients; NHS number and local patient identifiable codes; and anything else that may be used to identify a patient directly or indirectly.

[397] GMC, 'Confidentiality, Guidance for Doctors,' (12 October 2009) <http://www.gmc-uk.org/static/documents/content/Confidentiality_core_2009.pdf>

the public interest.[398] It further maintains that if information about a patient is disclosed, then it must be anonymised or coded.[399] Doctors must ensure that the patient is aware that their personal information might be disclosed and is given a chance to object.[400] If identifiable information is to be disclosed for purposes other than a patient's care or local clinical audit, then unless the disclosure is required by law or can be justified in the public interest, the patient must have expressly consented to such disclosure and the disclosure is required to be kept to the minimum necessary.[401]

Further, the Guidance provides that doctors must ensure that patients' personal information held or controlled by them is "effectively protected at all times against improper disclosure."[402] Also, expressly cautioned against is the sharing of identifiable information about patients where doctors may be overheard (e.g. in public places or Internet chat forums), sharing of passwords, leaving unattended patients' records (on or off screen) where they may be seen by other patients, unauthorised healthcare staff, or the public.[403]

More importantly, the Guidance also advocates the privacy of medical data and information in respect of it being shared with a patient's partner, carers, relatives or friends. Principle 64 provides that doctors must "establish with the patient what information they want you to share, who with, and in what circumstances," to ensure that a patient's need to keep their medical data and information private is assured. This establishes and confirms a default culture of non-sharing of information of highly sensitive nature – in this case medical data.

In the case of India, the situation is entirely different. There is routine, discriminate sharing of personal medical information and data in both public and private hospitals. Nagral recounts how in

[398] Principle 8
[399] Principle 9 (a)
[400] Principle 9 (b)
[401] Principle 9 (d)
[402] Principle 12
[403] Principle 13

> outpatient departments and operation theatres patients are forced to share all their unpleasant personal details not only with the doctor interviewing them but also with other doctors sitting across the table and other patients being interviewed by other doctors.[404]

Patients' personal information is indiscriminately used in public academic meetings and published in academic journals. Also shown is how, at medical meetings in Mumbai, doctors often in discussions of sensitive medical conditions like AIDS, photos of identifiable individuals are shown with no attempts to shield identity.[405] There is also no privacy for patients in respect of their personal information being released to their partners, carers, relatives or friends (in sharp contrast to UK practice).

Thus, it is evident that there are differences in the norms and conditions affecting the sharing of personal information (sensitive or otherwise) between the UK and India.

3.2.2.3.Communal use of personal information

It has been shown that privacy in terms of personal information exists very limitedly in India, and that personal information is habitually shared in manners far removed from the UK. In addition to this, there is another norm relevant to this research. This is the habitual communal use of personal information. The following examples illustrate this in the digital context.

The first is Hansdehar, India's first online knowledge village.[406] The village website functions as a "web interface for all stakeholders involved in the development and upliftment of the village." It has a comprehensive citizens' directory, a list of voters and a pensioners list. The village itself is not connected to the Internet and the villagers cannot browse the Internet or access the website. Yet, their personal data (name, date of birth, age, occupation, sex) is openly accessible and available on the

---

[404] A Nagral, 'Privacy in Public Hospitals' (1995) 3 (1) Indian Journal of Medical Ethics

[405] This despite the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, s 7.14 which states that a registered medical practitioner shall not disclose the secrets of a patient learnt in the exercise of professional duties except in a court of law under orders of the Presiding Judge, in circumstances where there is a serious and identified risk to a specific person and / or community and notifiable diseases. See Gazette of India, Part III, s 4 (6 April 2002).

[406] See <http://www.smartvillages.org/hansdehar/people.htm>

website. The goal in putting this information online was the collective good of the village - identified in this case, as the progress of the village and development of its infrastructure.

Here, the villagers have attained digital identities through their personal information being put online, in the interests of the collective good of the community. It is not known whether these villagers consented to the use of their personal information, though it is highly unlikely. Also, the question of consent might not arise because the information might not be viewed as 'personal' information in the strict sense of the term, as much of it exists in the public domain.

The next is the On Line Reservation Chart Display System implemented in Vadodara.[407] The system displays, on LCD screens at the Vadodara train station, online passenger reservation for a particular train. The screens broadcast passenger details – i.e., who is travelling, the status of their reservation, and the class of the train they will be travelling in. This is in keeping with the established trend of passengers' personal information (names, age, gender, boarding station, destination, seat number, and passenger-name record number) being published as a matter of routine policy at train stations and outside the train compartments. Passengers in India surveyed on this practice were found to have very low levels of concern about such practices.[408] Only 17 percent of Indian respondents expressed extreme concern over the posting, 23 percent were somewhat concerned, while the rest were either not very concerned (34 percent) or not concerned at all (26 percent).

The On Line Reservation Chart Display System is evidence of how habitually personal information is subject to public display by private or public entities providing services to individuals in India. Such uses of personal information have (as in the instant case) and will increasingly become part of the public domain in India.

---

[407] Express News Service, 'Computerised Chart Display System Arrives at Vadodara Railway Station,' (23 February 2009) <http://www.expressindia.com/latest-news/computerised-chart-display-system-arrives-at-vadodara-railway-station/426910/>

[408] P Kumaraguru & L Cranor, 'Privacy in India : Attitudes and Awareness" in G Danezis and D Martin (eds), *Privacy Enhancing Technologies, 5th International Workshop, PET 2005, Cavtat Croatia* (Springer, 2006)

This is very much evident in the case of the widespread availability of personal information of Indian voters online, in electoral voters lists published by State Commissions, fuelled by the need to publicise voter identities in the interests of ensuring the accuracy of voter identities and dissuading bogus voting.[409]

3.2.2.4.Attitudes to authentication and verification

Culture also impacts attitudes towards authentication and verification. This was substantiated in the context of biometric technology by Riley, Buckner, Johnson and Benyon.[410] In this study,[411] three countries were analysed: India, UK and South Africa.[412] There were two key research questions: first, to determine how biometrics was perceived in Western and developing cultures and second, to investigate the concerns of people in developing countries towards biometrics. The survey categories related to: knowledge of biometrics, the usability and reliability perceptions of biometrics, the acceptability of biometrics, fears or concerns about the technology and demographic questions.

The results were as follows. The Indian respondents led in their knowledge of biometrics, with South African respondents ranking second and the UK respondents ranking third. In relation to the perception of biometrics as a personal authentication mechanism (with regards to the use, speed of use and security of biometric technology), the Indian respondents gave biometrics the most positive rating while the British respondents gave it the least positive rating.[413] The Indian respondents expressed greater willingness to use biometrics as a means of personal authentication as compared to their British counterparts who found the idea less acceptable than other forms of authentication (e.g. authentication by password).[414] In regards to the

---

[409] JK Chopra, *Politics of Election Reforms in India* (Mittal Publications, Delhi 1989), 160
[410] Chris Riley, K Buckner, G Johnson and D Benyon, 'Culture & Biometrics: Regional Differences in the Perception of Biometric Authentication Technologies,' (2009) 24 (3) AI & Soc, 295–306
[411] The study makes a relation to Hofstede's cultural dimensions.
[412] India was chosen as an Asian example with huge market potential for biometrics, South Africa for its cultural and geographical divergence to India and the UK as an example of a 'developed European country.'
[413] Riley (2009) **n410**, 299
[414] Riley (2009) **n410**, 300

security of biometric information, the Indian and South African respondents were less concerned than the British.

The study thus demonstrates differences across cultures in attitudes to biometrics. The Indian respondents generally displayed a more favourable attitude to biometrics as compared respondents from the UK (with the least favourable view). While a third of the Indian respondents were largely unconcerned about the use of biometric systems, the British respondents were highly concerned about how biometric systems would be used and what their privacy impact would be.[415] In fact, privacy was a major concern of the British respondents in comparison to their Indian counterparts. The study broadly concluded that cultural differences had to be taken into account in the design and implementation of biometric systems. The results of this study are some evidence that local difference does affect how digital identity subjects relate to, experience and protect their digital identities - in this case their biometric identity.

Culture also influences attitudes towards other types of digital identity like smart cards. Though there are no UK-India specific comparative studies, there are other international studies that support this contention. For example, Hsu, Davison and Stares[416] and Bailey and Caidi.[417] Bailey and Caidi analysed attitudes to smart cards in two different cultures: Hong Kong Special Administrative Region (SAR) of the People's Republic of China and Ontario, Canada. They concluded that cultural and lifestyle norms like the non-prevalence of anonymity in Hong Kong and the open and transparent relationship between the public and the government led to positive attitudes in Hong Kong, as opposed to the negative attitude to smart cards in Ontario.[418]

The role of culture in the acceptance or rejection of means of identity authentication and verification is also evident in the comments made by the Privacy Commissioner

[415] This was a major concern of the British respondents. Riley (2009) **n410**, 303.
[416] Carol Hsu, R Davison and S Stares, 'Cultural Influences on Attitudes Towards Hong Kong's Smart Identity Card,' PACIS 2004 Proceedings, (2004), <http://aisel.aisnet.org/pacis2004/20>
[417] SGM Bailey and N Caidi, 'How Much Is Too Little? Privacy and Smart Cards in Hong Kong and Ontario,' (2005) 31 J of Info Sci, 354-364
[418] Bailey and Caidi (2005) **n417,** 356

of Italy in respect of identity cards and biometric identifiers. According to him, while identity cards were a part of Italian culture, but fingerprints as biometric identifier were not.[419] Thus, a form of identification, authentication and verification well received in one country might not be in another due to local cultural rejection of it.

There are of course at least two different manners in which the above findings could be understood. In the first interpretation, Western users are simply more aware of the inherent dangers of the abuse of their digital identity, more informed about the technology and its risks and hence more willing to pay a premium for its protection. Contrarily, Indian users may need education, awareness and 'protection for their own good' through technology or legal mechanisms, even if they currently experience this as protection of values they do not rate highly.

In the second interpretation, Europe and India display here a true divergence in ranking contingent social values, with both rankings just as valid. In much of the previous debate on digital identity regulation, the first interpretation dominated. Technological solutions such as identity management systems and legal mechanisms like privacy rights were promoted as universal goods and western-driven initiatives to support developing countries exported them globally. The interpretation proposed here is more nuanced, and while it does not subscribe to a radical form of value relativism (impossible for a global communication medium), it tries to give differences in value rankings a stronger voice.

3.2.2.5.Openness and transparency

Culture also determines to a fair extent openness and transparency in relation to digital identity. This is particularly evident in respect of digital identity mediated on social networking websites. This is substantiated by a survey conducted on international differences in the use of social networking websites by university

[419] See Communication by the Italian Privacy Commissioner in House of Commons Canada, 'A National Identity Card for Canada?' Report of the Standing Committee on Citizenship and Immigration (October 2003), 22 <http://oipc.bc.ca/pdfs/public/cimmrp06-e.pdf>

students in India and the United States.[420] Some of the findings are particularly telling and supportive of the claim that local difference affects digital identity.[421]

First, the study found that Indian students differ from their American counterparts in respect of the public and private nature of their profiles. 69.5 percent of the Indian students kept their profiles publicly visible while only a 28.6 percent (approximately a quarter) of American students did likewise. Second, in respect of making friends with unknown people (people not met before), it was found that 73.5 percent of the Indian students had online friends they had not met previously. In comparison, 77.5 percent of American students had no online friends they had not met before. Third, the Indian students (25.4 percent) were far more communicative on social networking sites about health issues as compared to their American counterparts (8.9 percent). These findings are particularly relevant to demonstrate that there are differences in how individuals mediate their digital identities- whether digital identities are open and transparent or closed and non-transparent.

3.2.2.6.Anonymity and pseudonymity

Local difference is also evident in digital anonymity and pseudonymity in the UK and India.

In the digitally advanced West, anonymity and pseudonymity are generally accepted, particularly in the online context, as pillars of privacy and data protection that enable digital identity subjects have autonomy over their digital identities.[422] In the US, the characterisation has been made that "anonymity rules"[423] supported by the legal system. Fertik and Thompson call it the "culture of anonymity."[424] In the EU too, there is strong support for anonymity and pseudonymity as essential to the

---

[420] BA Marshall and ors, 'Social Networking Websites in India and the United States: A Cross-National Comparison of Online Privacy And Communication' (2008) 9 (2) Iss in Info Systems, 87-94
[421] 245 Indian and 241 American university students were surveyed about their attitudes to privacy and communication patterns on social networking sites.
[422] See Pfitzmann (2008) **n151**; Stefanos Gritzalis, 'Privacy Issues in the Digital Era,' Guest Editorial, (2006) 16 (2) Internet Research, 117
[423] Michael Fertik, David Thompson, *Wild West 2.0: How to Protect and Restore Your Online Reputation on the Untamed Social* (Amacom, NY 2010), 61
[424] Fertik (2010) **n423**, 74

advancement of the digital identity subjects rights and the autonomy of the individual.[425]

Anonymity and pseudonymity are often expressed in the digital identity context in the use of PETs.[426] Though questions have been raised about their effectiveness in protecting digital identity,[427] their usefulness is still widely accepted in the digitally advanced West.[428] A survey of European data controllers found that nearly half the respondents (52 percent) used PETs in their organisation.[429] The UK ICO also advocates the use of PETs.[430]

The culture of privacy and data protection in the UK promotes the expression of anonymous and pseudonymous digital identities. The law too, supports the

---

[425] See the Ministerial Declaration of the Ministerial Conference in Bonn on Global Information Networks, 6-8 July 1997; EC Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Recommendation 3/97: Anonymity on the Internet, Adopted on 3 December 1997, XV D /5022/97 final WP 6; Kokswijk (2007) **n262**, 210

[426] David Chaum, 'Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms,' (1981) 24 (2) Communications of the ACM, 84-90; David Chaum, 'Security Without Identification: Transaction Systems to Make Big Brother Obsolete,' (1985) 28 (10) Communications of the ACM, 1030-1044; A Pfitzmann, M Waidner, 'Networks Without User Observability: Design Options,' in F Pichler (ed), *Advances in Cryptology, EUROCRYPT '85: Proceedings of a Workshop on the Theory and Application of Cryptographic Techniques* (Springer, Berlin 1986), 245-253; A Pfitzmann, B Pfitzmann and M Waidner, 'ISDN-mixes: Untraceable Communication With Very Small Bandwidth Overhead' in W Effelsberg, HW Meuer and G Müller (eds), *Proceedings of the GI/ITG Conference on Communication in Distributed Systems* (Springer, Germany 1991), 451-463; DM Goldschlag, MG Reed and PF Syverson, 'Hiding Routing Information,' in R Anderson (ed), *Information Hiding* (Springer, Berlin 1996), 137-150; J Camenisch and EV Herreweghen, 'Design and Implementation of the *idemix* Anonymous Credential System,' in V Atluri (ed), *Proceedings of the 9th ACM Conference on Computer and Communications Security CCS'02* (ACM Press, NY 2002), 21-30; GW Blarkom, J Borking and J Olk, *Handbook of Privacy and Privacy-Enhancing Technologies* (College bescherming persoonsgegevens, The Hague 2003)

[427] Felix Stalder, 'The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy,' (2002) 7 (2) Sociological Research Online, <http://www.socresonline.org.uk/7/2/stalder.html>

[428] John Borking, 'The Use and Value of Privacy-enhancing Technologies,' in Susanne Lace (ed), *The Glass Consumer: Life in a Surveillance Society* (Policy Press, Bristol 2005), 69-98; John Borking and C Raab, 'Laws, PETs and Other Technologies for Privacy Protection,' 2001 (1) JILT <http://elj.warwick.ac.uk/jilt/01-1/borking.html; Vanja Senicar, Borka Jerman-Blazic and Tomaz Klobucar, 'Privacy-Enhancing Technologies: Approaches and Development,' (2003) 25 (2) Computer Standards & Interfaces, 147-158

[429] The Gallup Organisation, Data Protection in the EU: Data Controllers' Perceptions (EC Flash Barometer No 226), Brussels (17 April 2008) <http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf>. The survey involved 4,835 randomly-selected data controllers in 27 EU Member States.

[430] ICO, Privacy Enhancing Technologies (PETs), Data Protection Technical Guidance Note, (2006) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies.pdf>

expression of anonymous and pseudonymous digital identities to the extent that no illegal acts are committed.[431] Digital identity subjects are aware of and use anonymous and pseudonymous services. They also employ more traditional means of expressing anonymity and pseudonymity like providing incorrect information in relation to their identities to shield them from discovery.[432]

In India, the situation is complex. On the one hand, traditional culture offers robust support for anonymity and pseudonymity.[433] Folklore and religion are full of examples of heroes or deities either intentionally hiding their true self to achieve a (more or less) praiseworthy goal, or, in the form of *Avatars* using different identities as a matter of course. Indeed, the most iconic expression of digital identity, the *Avatar*, is rooted in Hinduism.[434] According to the *Bhagavata Purana*, the Lord Vishnu's *Avatars* are innumerable,[435] and while the term is mostly used with relation to him, other deities like Ganesha[436] and Shakti also have *Avatars.*[437]

However, in the context of digital identity little recourse seems to be made to this religious archetype. What seems more influential is the traditional tenet of 'Self as Consciousness' embodied in Book III, Part 1 of the *Mundaka Upanishad*[438] which states,[439]

> By truthfulness,
> By restraint,
> Right knowledge,
> Austerity,

---

[431] See First Report on the implementation of the Data Protection Directive, COM (2003) 265(01), (15 May 2003), <http://eurlex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf>; WP 37 of the Article 29 Working Party, 'Privacy on the Internet - An Integrated EU Approach to On-line Data Protection,' (November 2000) <http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2000/wpdocs00_en.htm>

[432] Ronald Leenes and Isabelle Oomen, 'The Role of Citizens: What Can Dutch, Flemish and English Students Teach Us About Privacy,' in S Gutwirth and ors (eds), *Reinventing Data Protection* (Springer Verlag, NY 2009), 149

[433] Rodrigues (2008) **n278**

[434] First used in the online context by Neal Stephenson in his novel Snow Crash (drawn from the Sanskrit *Avatāra* meaning an incarnation of a deity).

[435] G Somany, *Vishnu and His Avatars,* (Bookwise, India 2004)

[436] JA Grimes, *Ganapati: Song of the Self* (SUNY Press, Albany1995), 105

[437] Geoff Teece, *Hinduism,* (Franklin Watts, London 2003), 8

[438] The Upanishads are a key element of Vedic philosophy and the Mundaka Upanishad is one of the primary Upanishads derived from the *Atharvaveda.*

[439] Per A Jacobs, *The Principal Upanishads: The Essential Philosophical Foundation of Hinduism* (Watkins Publishing, London 2008), 162.

> The recognition of one's own
> Self as Consciousness,
> Awareness and Love
> is gained,
> 'That' which pure…

According to this passage, an individual attains the highest level of fulfilment when the Self is consciously recognised. There is need for oneness with the Self, in the forms it manifests. Thus this leaves no scope for falsehoods, such as might be manifest in anonymity and pseudonymity.[440] In the case that falsehoods are made, they are sign of individuality which would lead to the non-achievement of the *Atman*[441] or the higher purpose of existence in Hinduism.

This might be a factor that leads digital identity subjects in India to exercise anonymity and pseudonymity in digital identities, exceptionally and in a limited manner. It might also account for the general governance policy that does not advocate or promote the achievement of anonymity[442] and pseudonymity[443] in digital contexts-exemplified in the resistance to technologies that enhance these.[444] For instance, the legal restrictions applicable in respect of cryptography,[445] and the attempts by the Indian government to get Blackberry to enable access to its encrypted BlackBerry Enterprise Server email service.[446]

---

[440] This is because falsehood fosters individuality or "ego centric personality." See Swami Krishnananda, *The Mundaka Upanishad*, (Divine Life Society, Sivananda Ashram), 2 <http://www.sankaracharya.org/library/mundaka.pdf>

[441] In Hindu philosophy, *Atman* refers to the true self. See Anmol Publications, *The Encyclopedia of Hinduism* (Anmol Publications, New Delhi 2000), 94

[442] **Ch 6 (6.3.4.2)**

[443] **Ch 6 (6.3.5.2)**

[444] N Shah, 'Subject to Technology: Internet Pornography, Cyber-Terrorism and the Indian State,' (2007) 8 (3) Inter-Asia Cultural Studies, 349-366

[445] Nehaluddin Ahmad, 'Restrictions on Cryptography in India: A Case Study of Encryption and Privacy' (2009) 25 (2) CLSR, 173-180

[446] 'India Gives BlackBerry More Time,' *The Telegraph* (31 Aug 2010) <http://www.telegraph.co.uk/technology/blackberry/7972926/India-gives-BlackBerry-more-time.html>. The government of India has also attempted similar moves with Google and Skype. S Sahu and R Guha, 'India Wants to See Google, Skype Data,' *The Wall Street Journal* (2 September 2010).

The dichotomy between the two religious narratives[447] allows us to exemplify the main argument of this thesis. Some legitimate identity concerns in India could be addressed by a more permissive use of *avatars* as multiple, pseudonymous online identities.[448] This is presently 'blocked' also by the "self-as-consciousness" narrative cited above, and the more mundane power interests of the State that uses them. Our approach can get traction, match local understandings and thus support, if it is embedded in the competing narrative of divine *avatars* that is suggested here as a tool to be pushed to rebalance risk allocation in digital interactions.

However, these *avatars* are not a one-to-one translation of their popular MMORPG counterparts. Indeed, Stephenson's use of the term has only superficial similarity with the meaning of the concept in Hinduism. Rather than an arbitrary collection of otherwise unconnected identities, *avatars* and their substratum are in a radical sense identical – manifestations of an underlying oneness rather than totally independent incarnations and diversity[449] which therefore, in more pragmatic legal terms, can always be traced back to its underlying reality.

Avatars in their religious origin are also 'function specific.' A central passage from the *Bhagvadgita* describes the typical role of an *Avatar* of Vishnu as bringer of *dharma* or righteousness back to a disturbed social order:

> Whenever righteousness wanes and unrighteousness increases I send myself forth. For the protection of the good and for the destruction of evil, and for the establishment of righteousness, I come into being age after age.[450]

This moral imperative in the very definition of an *Avatar* bridges the gap between the more permissive use of *avatars* advocated here, and the moral ideal expressed in the *Mundaka Upanishad*. *Avatars* are only legitimate if embedded in a system of rightful

---

[447]The free expression of identities in *Avatars* and the 'Self as Consciousness' in the *Mundaka Upanishad.*

[448] By using the traditional religious concept of the Avatar as something designed to be moral, a legitimate use of pseudonymity can be found grounded in culture. This use would carry limits and be grounded in the "collective interest" and hence subject to appropriate social and legal restrictions.

[449] Freda Matchett, *Krsna: Lord or Avatara? The Relationship between Krsna and Vishnu* (Curzon Press, Surrey 2001). In Christianity, the (heretical) doctrine of docetism comes closer to the meaning than a translation as incarnation. See EG Parrinder, *Avatar and Incarnation* (Oneworld Publications, London 1997), Ch 17, 240-250

[450] The *Bhagvadgita*, 4, 7–8

behaviour, their use is not an unfettered right, but coordinated with a complex set of duties and expectations. In chapter 8, this approach will be generalised further in a duty-centric notion for digital identities. What we can see in the *Avatars* example is how this can play out in protecting Indian identity subjects against threats to their digital identity while at the same time staying true to a well understood system of norms and values that is not simply a copy of the Western notion.

3.3. Conclusion

This chapter set forth the local context of digital identity, in two main respects: state of digital technology and culture.

In the context of digital technology, there are vast differences between the UK and India in respect of the operating conditions, penetration, access and use. This, as will become evident as the thesis progresses, is highly relevant to how digital identities are managed and regulated. Regulation that works well in an environment of high penetration and high access is not necessarily suitable, and can even be counterproductive, in an environment marked by limited access, low penetration and infrequent use.

In the context of culture, it is clear that culture (in the shape of attitudes, social values, norms and practices) influences how individuals relate to, express, use and protect their digital identities.[451] This was demonstrated in various contexts (like privacy, information sharing, communal use of personal information, authentication and verification, openness and transparency, anonymity and pseudonymity) with suitable digital examples that show sharp contrasts between the UK and India

[451] A view supported by Kendall who postulated that culture, amongst other things is a prominent factor in the formation of digital relationships. L Kendall, 'Meaning and Identity in "Cyberspace": The Performance of Gender, Class, and Race Online,' (1998) 21 Symbolic Interaction, 129-53.

4. Digital identity management: The technical regulation of digital identity

> The Gileadites captured the fords of the Jordan leading to Ephraim, and whenever a survivor of Ephraim said, "Let me cross over," the men of Gilead asked him, "Are you an Ephraimite?" If he replied, "No," they said, "All right, say 'Shibboleth.'" He said, "Sibboleth," because he could not pronounce the word correctly, they seized him and killed him at the fords of the Jordan. Forty-two thousand Ephraimites were killed at that time.
> *-Judges 12:5-6*[452]

> Since the adorable sun-god, wind-god, the four quarters and even so the moon-god, as also the deity presiding over the day-time and the twilights and the night and the earth and even others know me to be endowed with good conduct, so let the fire-god protect me. Thus speaking, Seetha walking around the fire-god, with her mind free from hesitation, entered the blazing fire. Then, the fire-god, the witness of the whole world, spoke to Rama as follows "Here is your Seetha. No sin exists in her." "This auspicious lady, whose character has been good, has never been unfaithful to you who are endowed with strength of character either by word or by mind or even by intellect or by her glances." "Take back Seetha, who is sinless, with a pure character.
> *- Yuddhakanda (Book of War)*[453]

4.1. Introduction

In the opening quotes of the chapter, two different instances of identity management are evident. In the first, the Gileadites use pronunciation abilities as a means of authenticating identity and ensuring border control. In the second, Seetha verifies her identity as a pure and virtuous woman by taking the fire test. Both are examples of different forms of identity management, which demonstrate that there can be many contexts of identity management.

Identity management, a regular life occurrence, takes places in different contexts and conditions. There are numerous examples of identity management: Wearing a wedding band or *mangalsutra*[454] to signify marital status. Parents introduce their children to their friends. Artists sign their paintings. Writers use pseudonyms. Robbers or bandits wear masks. Makeup is worn to hide age lines. Code names are used in love letters. Fingerprints are used to verify identity. Changing one's name or

[452] Zondervan Publishing, *The Bible:New International Version* (Zondervan Publishing, Grand Rapids 2003)
[453] Chapters 116 and 118 of the *Ramayana.* Translation by KMK Murthy. At <http://www.valmikiramayan.net/>
[454] A sacred thread worn as a signifier of Hindu and Syrian Christian marriage in India.

sex. The list is inexhaustible. From these instances, it is evident that identity management has many elements: identity creation, classification, affiliation, authentication, verification, privacy, anonymity, pseudonymity, security and identity destruction.

This chapter examines digital identity management, the technical regulation of digital identity, which emerged particularly in the digitally advanced West as an industry self-regulatory solution for the creation, control and management of digital identities. It is globally marketed as a means that will enable digital identity subjects control their digital identities. But, does digital identity management measure up as an effective regulator of digital identity? More crucially, does it take into account the global and simultaneously local contexts of digital identity?

4.2. Digital identity management: Its development

The Internet, as originally conceived and built, was not equipped for identity management. It had no identity layers; as Peter Steiner put it, "On the Internet, nobody knows you're a dog."[455] With the increasing uptake, commercialisation and globalisation of the Internet, this state of affairs was no longer found to be satisfactory for a number of reasons, key amongst which were: trust, the challenge of multiple digital identities,[456] fraud, security, privacy and data protection concerns.

The trust issue was a key basis on which initial identity management technologies were pushed forward. Trust is a key feature of digital identity transactions.[457] Identity subjects need to be able to trust their identity providers or other digital identity subjects and vice versa. Service providers needed to be able to trust their digital identity subjects. At all levels, a need was felt to 'know the identity' to be able to deal with or conduct a successful transaction with the identity.[458]

---

[455] P Steiner, *The New Yorker* (5 July 1993) 69 (20)
[456] See **Ch 2 (2.5.1)**
[457] Piotr Cofta, *Trust, Complexity and Control: Confidence in a Converged World* (John Wiley, Chichester 2007)
[458] Mary Rundle and B Laurie, 'Identity Management as a Cybersecurity Case Study,' OII Conference on Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities, Research Publication No 2006-01, (2005) <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2006_01_Rundle_IdentityManagement_CybersecurityCaseStudy.pdf>

Another thrust to identity management was the need to control and manage multiple identities[459] as they created problems of accountability, accuracy, authentication and trust,[460] dispersion, interoperability[461] and management. [462] Hence, solutions were put forth to deal with these problems.

Fraud and security concerns also contributed to the advancement of digital identity management. As digital identities became popular and widespread across domains and their social and civil significance increased, they gained significant economic and non-economic value, particularly in the digitally advanced West.[463] This made digital identity the new crime frontier.[464] Digital identities became increasingly susceptible to fraud (e.g. impersonation, deception, usurpation and phishing[465]), social engineering and hacking. Therefore, a need was felt to manage and secure digital identities against threats to and from them, through their proper administration, authentication, and security.[466]

Privacy and data protection were other key factors that stimulated, boosted and continue to propel the development and uptake of digital identity management,

---

[459] Ahto Buldas, P Laud and H Lipmaa, 'Accountable Certificate Management Using Undeniable Attestations,' in Pierangela Samarati (ed), *Proceedings of the 7th ACM Conference on Computer and Communications Security* (ACM, NY 2000), 9-17; DA Buell & R Sandhu, 'Identity Management,' (2003) 7 (6) IEEE Internet Computing, 26-28; E Damiani, S. De Capitani di Vimercati, P Samarati, 'Managing Multiple and Dependable Identities,' (2003) 7 (6) IEEE Internet Computing, 29–37.
[460] S Xu, R Sandhu and E Bertino, 'TIUPAM: A Framework for Trustworthiness-Centric Information Sharing,' in Elena Ferrari and ors (eds), *Trust Management III,* IFIP AICT 300 (Springer, Germany 2009), 164-175, 170
[461] Windley (2005) **n122**, 118
[462] Birch (2007), **n122,** 110, 183
[463] Corien Prins, 'Property and Privacy: European Perspectives and the Commodification of Our Identity,' in L Guibault and PB Hugenholtz (eds), *The Future of the Public Domain* (Kluwer Law International, The Netherlands 2006), 223–257 (personal data as commercially valuable asset); J Litman, 'Information Privacy/Information Property,' (2000) 52 Stan LR, 1283-1313, 1290; KC Laudon, 'Markets and Privacy,' (1996) 39 Communications of the ACM, 93, 103; A Bartow, 'Our Data, Ourselves: Privacy, Propertization, and Gender,' (2000) 34 U San Francisco LR, 633-704, 695
[464] See US Federal Trade Commission, Identity Theft Survey Report, 7 (2003); CIFAS, Fraud Trends, 2006-2010 <http://www.cifas.org.uk/default.asp?edit_id=562-57>; CIFAS, 'The Anonymous Attacker: A Special Report on Identity Fraud and Account Takeover,' (2009), <http://www.cifas.org.uk/download/The_Anonymous_Attacker_CIFAS_Special_Report.pdf>; WenJie Wang, Yufei Yuan, Norm Archer, 'A Contextual Framework for Combating Identity Theft,' (2006) 4 (2) IEEE Security & Privacy, 30-38
[465] Francois Paget, 'Identity Theft,' Technical White Paper No 1, (McAfee, 2007)
[466] Rundle (2005) **n458**

particularly in the digitally advanced West.[467] The need of identity subjects[468] to "determine for themselves when, how and to what extent information about them is communicated to others,"[469] bolstered the development of identity management solutions with a strong and overt focus on privacy and data protection. For example, PETs.[470]

The Internet advanced from a "no one knows" Internet, as Lessig termed it,[471] to an all-knowing Internet, to enable greater security (that was the primary rationale). Identity got layered into the Internet in the form of IP addresses, cookies, encryption, amongst other things.[472] All this was done to enable greater transparency, accountability and responsibility (TAR) in relation to digital identities. This TAR movement gave rise to distinct entities called identity providers or entities that issue and/or authenticate digital identities.

The Article 29 Data Protection Working Party highlighted the expansion of digital authentication services as a factor that changed the digital landscape, particularly in regards to its implications for digital identity subjects, who were now expected to register, identify and authenticate themselves to access and use services.[473] In effect,

---

[467] See Elisa Bertino and Jason Crampton, 'Security for Distributed Systems: Foundations of Access Control,' in Yi Qian, D Tipper, P Krishnamurthy and J Joshi (eds), *Information Assurance: Dependability and Security in Networked Systems* (Morgan Kaufmann Publishers, San Francisco 2008), 74 (strong links between privacy and identity management); J Dumortier and C Goemans, 'Privacy Protection and Identity Management,' in B Jerman-Blažič, W Schneider and T Klobučar (eds), *Security and Privacy in Advanced Networking Technologies* (IOS Press, Netherlands 2004), 191-212 (privacy legislation as driver for IM); Ronald Leenes, J Schallaböck and M Hansen (eds), 'Privacy and Identity Management for Europe,' PRIME Whitepaper, Ver. 2, (June 2007) <www.prime-project.eu/ prime_products/whitepaper>

[468] Oliver Berthold and Martin Kohntopp, 'Identity Management Based on P3P,' in Hannes Federrath (ed), *Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability* (Springer, Berlin 2001), 141-160, 142. Also Kokswijk (2007) **n262**, 164

[469] Westin (1967) **n348**

[470] A Bhargav-Spantzel, AC Squicciarini, M Young and E Bertino, 'Privacy Requirements in Identity Management Solutions,' in MJ Smith and G Salvendy (eds) *Human Interface and the Management of Information: Interacting in Information Environments Part II* (Springer, Berlin 2007), 694-702; Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato & Leonardo Martucci (eds), *The Future of Identity in the Information Society* (Springer, USA 2008)

[471] Lessig (2006) **n151,** 35

[472] Lessig (2006) **n151**

[473] Article 29 Data Protection Working Party, 'Working Document on On-line Authentication Services,' Adopted on 29 January 2003, Brussels, 10054/03/EN, WP 68

the development of identity management began in earnest with cryptographic tools like digital signatures and digital certificates.

4.2.1. Digital Signatures

Digital signatures,[474] an expression of public key cryptography or asymmetric cryptography, are digital codes attached to electronically transmitted documents to verify their contents and the sender's identity.[475] The concept of digital signatures was proposed by Diffie and Hellman in 1976 to support authentication in ecommerce - as a safeguard to prevent disputes between transacting entities.[476]

Traditional cryptographic systems work on the basis of shared key management (also called secret key or symmetric cryptography). In this case, the sender and receiver of a message use a like key at both ends to encrypt or decrypt messages. Asymmetric or public key cryptography works differently to traditional or symmetric cryptography. In public key cryptography, both the sender and the receiver of a message get a pair of keys - a secret private key and a public key, both of which are linked to one another mathematically.[477]

Rivest, Shamir and Adleman built on the Diffie-Hellman concept and developed the RSA algorithm.[478] Along with the Digital Signature Algorithm (DSA), the RSA algorithm remains the most widely adopted. The DSA was specified as the Digital Signature Standard by the US National Institute of Standards and Technology (NIST)[479] and envisaged as suitable in a variety of applications like electronic funds

---

[474] For a detailed technical overview of digital signatures see Jonathan Katz, *Digital Signatures* (Springer, NY 2010), Stephen Paine and Mohan Atreya, *Digital Signatures* (McGraw Hill/Osborne, USA 2002).
[475] These are sometimes used to implement electronic signatures.
[476] W Diffie and ME Hellman, 'New Directions in Cryptography,' (1976) IT-22 (6) IEEE Transactions on Information Theory, 644-654
[477] For further details of how public key cryptosystems and digital signatures work, see RSA Labs, 'Public-Key Cryptography Standards (PKCS),' Chapter 2, <http://www.rsa.com/rsalabs/node.asp?id=2165>
[478] RL Rivest, A Shamir and L Adleman, 'A Method For Obtaining Digital Signatures and Public-Key Cryptosystems,' (1978) 21 (2) Communications of the ACM, 120–126
[479] Fact Sheet On Digital Signature Standard (May 1994)

transfer systems, Electronic Data Interchange (EDI), distribution of software, and guaranteeing database integrity.

Digital signatures work as follows: first, they verify the genuineness of the origin of the message and second, they corroborate the validity of the data message. While digital signatures were perceived and created as digital equivalents of their paper counterparts, they differ. While a paper based signature is visible instantly on its medium (the paper), digital signatures are not. Digital signatures only become apparent when presented on a computer screen or printout.[480]

4.2.2. Digital Certificates

Digital certificates[481] proliferated as means of boosting trust in digital transactions. They are electronic documents utilised to identify individuals, servers, companies or entities and to associate that identity with a public key.[482] They are issued by independent trusted parties called Certification Authorities (CA's) to certify the true identity of an entity. Before a CA can issue a digital certificate to any party, it must validate the identity of the party making the request for the certificate according to its own policy, which it must publish so that a person relying on that certificate is aware of the certification procedures and can make a judgment about accepting or rejecting the digital certificate.[483]

The manner in which a digital certificate works is simple: When one tries to connect to a website through Internet Explorer, that website's digital certificate is activated. Internet Explorer checks the certificate for any trust and security issues and if any are found, rejects the connection. If no issues are found and the certificate is approved,

---

[480] Audun Jøsang, D Povey and A Ho, 'What You See is Not Always What You Sign,' Proceedings of the Australian Unix User Group Symposium, Melbourne (September 2002), <http://persons.unik.no/josang/papers/JPH2002-AUUG.pdf>

[481] For detailed analysis, see Jahal Feghhi, Peter Williams, Jalil Feghhi, *Digital Certificates: Applied Internet Security* (Pearson Education Limited, Harlow 1998); SA Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy* (The MIT Press, 2000)

[482] As defined by Sun Microsystems Inc, *Sun Java System Access Manager 7.1 Federation and SAML Administration Guide* (Sun Microsystems, Santa Clara 2007), 274

[483] A Torrubia, FJ Mora, L Marti, 'Cryptography Regulations for E-commerce and Digital Rights Management,' (2001) 20 (8) *Computers & Security*, 724-738

the connection is made. Thus digital certificates are a guarantee and means of determining the legitimacy of digital identity.

All these developments explain the push towards digital identity management. To a great extent though, the continued sustenance of digital identity management, lies in the privacy and data protection thrust of the digitally advanced West which provided the impetus and is constantly employed as the primary marketing strategy for developing and promoting identity management solutions,[484] not just in the digitally advanced West but all across the world.[485]

4.3. Digital identity management: The market

Digital identity management is big business. It was estimated by Forrester Research, that the global identity management market (in this context, the identity and access management market) is expected to expand from 2.6 billion dollars (£1.65 billion) in 2006 to 12.3 billion (£7.84 billion) in 2014.[486]

The OECD Working Paper on Personhood and Identity[487] also predicted a growth in the demand for digital identity management solutions and envisaged a dramatic increase in consumer demand for privacy and protection from identity fraud. It declared that there would be a "competitive necessity" that leads businesses to create identity management partnerships in the operation of their digital services.

---

[484] PricewaterhouseCoopers and ITGI, *Enterprisewide Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment* (ISACA/ITGI, USA 2003), 19, 27 (identity management strengthens privacy); Jan Camenisch and ors, 'Privacy and Identity Management for Everyone,' in *Proceedings of the Workshop on Digital Identity Management* (ACM, NY 2005), 20-27; P Guarda and N Zannone, 'Towards the Development of Privacy-Aware Systems,' (2009) 2 Information and Software Technology, 337-350

[485] Brian Fonseca, 'New Identity Management Products Abound,' *Infoworld* (20 June 2003); M Casassa Mont, 'Dealing with Privacy Obligations: Important Aspects and Technical Approaches,' in Sokratis Katsikas, J Lopez and G Pernul, *Trust and Privacy in Digital Business* (Springer, Berlin 2004), 120–131; DM Goldschlag, MG Reed, 'Onion Routing For Anonymous and Private Internet Connections,' (1999) 42 (2) Communications of the ACM, 84–88

[486] This figure includes revenues from both implementation services and products. A Cser and J Penn, 'Identity Management Market Forecast: 2007 To 2014: Provisioning Will Extend its Dominance of Market Revenues,' Forrester Research (6 February 2008) <http://www.forrester.com/Research/Document/Excerpt/0,7211,43842,00.html>

[487] OECD (2007) **n140**

Most major international computer and software corporations like EMC (RSA), Google, IBM, HP, Microsoft, Novell, Oracle, Sun Microsystems, and Yahoo! are key identity management solution providers, either by themselves or as part of massive identity associations or conglomerates. Huge investments have been made into the digital identity markets and research and development. Global identity alliances (the OpenID Foundation, Information Card Foundation[488]) and mergers have occurred (e.g. Yahoo! and Flickr in 2005, Google and YouTube in 2006, LiveJournal and SUP in 2007) in an effort to tap the huge potential of the identity markets.[489]

But digital identity management is not big business just in the private sector. In the UK public sector, a Home Office Report[490] estimated that for providing identity cards to foreign nationals applying to extend their leave in the UK from October 2009 to October 2019 the cost was estimated at a total of £309 million (including set up costs of £28m and operational costs of £281 million).[491]

The digital identity market has also been visualised as having great potential in India.[492] The uptake of digital identity management solutions has shown some growth in the commercial and non-commercial sectors. But, it is a relatively new market and particularly growing in relation to a need and demand for security, rather than privacy.[493]

---

[488] Made up of Equifax, Google, Microsoft, Novell, Oracle, PayPal and others.
[489] For instance, Microsoft bought U-Prove. K Cameron, 'Microsoft to Adopt Stefan Brands' Technology' (6 March 2008) <http://www.identityblog.com/?p=934>. Oracle has acquired Sun Microsystems, see A Clark, 'Oracle's takeover of Sun Microsystems comes as surprise to software industry,' *The Guardian* (20 April 2009) < http://www.guardian.co.uk/business/2009/apr/20/sun-microsystems-oracle-takeover>
[490] Home Office (IPS), 'National Identity Service Cost Report: October 2009,' Presented to Parliament Pursuant to Section 37 of the Identity Cards Act 2006 <http://www.ips.gov.uk/cps/files/ips/live/assets/documents/IPS_Cost_report_2009_v5.pdf>
[491] The costs include provision for optimum bias.
[492] Infosecurity, 'Access and Authentication Market: Ready to Meet Tomorrow's Critical Needs?' techFocus, *InfoSecurity* (January 2009) <http://fanaticmedia.com/infosecurity/archive/Jan%2009/Authentication%20Market.htm>
[493] Nivedan Prakash, 'Building a Holistic Security Approach,' *Express Computer* (29 March 2010) <http://www.expresscomputeronline.com/20100329/20thanniversary07.shtml>; Infosecurity, 'Access and Authentication Market: Ready to Meet Tomorrow's Critical Needs?' *InfoSecurity* (January 2009) <http://fanaticmedia.com/infosecurity/archive/Jan%2009/Authentication%20Market.htm>

The growth in the commercial identity management sector in India, unlike the specific local need based (referring largely here to privacy and data protection) development in the UK can also attributed to a 'keeping the trade' rationale.[494] Organisations in India, particularly in the outsourcing industry, are implementing identity management solutions to comply with expectations of digital identity subjects that have their identities outsourced and the laws of the countries outsourcing the identities. This is evident in the following statement on the issue:

> Identity management applications enable organisations to provide policy based, auditable access to their IT systems. This also helps them in complying with several US, Europe and local regulations that require them to prove that their businesses are adequately protected. [495]

The one context where local need based identity management does manifest itself is in the implementation of the UID project, India's national identity system.[496] The system aims at providing a unique identity number to Indian residents, collecting and managing demographic and biometric information, ensuring non-duplication of identity, and offering "anytime, anywhere, anyhow" authentication of identity to users and service providers.[497]

4.4. Digital identity management: Defined and analysed

Digital identity management has been variously defined by technical and academic writers. According to Windley, digital identity management is "creating, managing, using and eventually destroying records…"[498] Rundle and Laurie describe identity management as referring to the "administration of authentication, access restrictions, passwords, access rights, account profiles, and other points of control for that

---

[494] See statement of T Srinivasan, Country Manager, Software for HP India Sales in relation to the uptake of identity management solutions in India, "…India has a track record of adopting global trends in software tools and technologies at a fast pace. While no syndicated reports on market size exist, trends are available specifically for India; one can expect encouraging growth here." Reported at C Jena, 'It's All About Identity,' *Express Computer* (19 February 2007) <http://www.expresscomputeronline.com/20070219/market02.shtml>
[495] <http://www.expresscomputeronline.com/20070219/market02.shtml>
[496] For details of the UID Scheme, see <http://uidai.gov.in/>
[497] UIDAI, 'Aadhaar-Communicating to a Billion: An Awareness and Communication Report,' ACSAC (17 May 2010) <http://uid-india.com/Documents/AADHAAR_CommPDF.pdf>
[498] Windley (2005) **n122,** 8

identity."[499] Cavoukian explains identity management (technology based) as being, "the administration and design of identity attributes, credentials and privileges."[500]

Pato defines identity management as a "set of processes, tools and social contracts surrounding the creation, maintenance and termination of a digital identity for people or, more generally, for systems and services to enable secure access to an expanding set of systems and applications."[501] Hansen defines identity management as, "managing various partial identities (usually denoted by pseudonyms) of an individual i.e. administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role."[502]

Though digital identity management has thus been defined in different manners,[503] it mainly involves the administration of digital identities such that it enables control over them.

From the stakeholder perspective, digital identity management can be categorised into three non-exclusive[504] levels: organisational, governance and individual. Organisational and governance based identity management fall into the category of other based identity management (management of digital identity by someone other

---

[499] Rundle (2005) **n458**

[500] A Cavoukian, '7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age,' Whitepaper, Information and Privacy Commissioner of Ontario, (2006) <http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf>

[501] J Pato, 'Identity Management: Setting Context,' *Encyclopedia of Cryptography and Security*, (Summer/Fall 2003) <http://www.hpl.hp.com/techreports/2003/HPL-2003-72.pdf>

[502] Pfitzmann (2008) **n151**

[503] For more definitions see J Bamford, 'Identity Management: Achieving Data Protection Compliance and Inspiring Public Confidence,' Position Paper for the Forum on E-Infrastructures for Identity Management and Data Sharing, OII, (2007); M Crompton, 'Proof of ID Required? Getting Identity Management Right,' Australian IT Security Forum (30 March 2004), 1; A Scorer, 'Identity Directories and Databases,' in DGW Birch (ed) *Digital Identity Management: Technological, Business and Social Implications* (Gower, Hampshire 2007), 41-49, 43; S Brands, 'Secure Access Management: Trends, Drivers and Solutions,' (2002) 7 (3) Information Security Technical Report, 81-94, 81; A Jøsang and ors, 'Trust Requirements in Identity Management,' in R Buyya and ors (eds) *Proceedings of the 2005 Australasian Workshop on Grid Computing and E-research:Vol 44* (ACS, Australia 2005), 99-108, 99

[504] Non-exclusive as the three categories overlap and mutually co-exist.

than the digital identity subject) and individual identity management falls into the category of self-management (management by the digital identity subject itself). [505]

Organisational digital identity management refers to identity management by an organisation in the context of that organisation's activities. An organisation may manage identity for a number of reasons: efficient business management, securing access to resources, user/employee account management, reduction of costs, to deter fraud, reduce data protection breaches, manage reputation, financial or other risk, or to enable profiling for market research. This kind of identity management is carried out by identity or service providers.[506]

Like the Gileadites, States are actively involved in digital identity management. This *governance* based identity management is justified by the argument that it enables States effectively govern through knowing their subjects and thus helping regulate their behaviour.[507] It is also justified on grounds that it enables the State to determine the rights and privileges of the people it governs and to maintain national security through securing borders and in enforcing border control (this is the area with the largest identity management impact). Examples that fit into this category are national identity systems and biometric border control systems.

Identity management also occurs at the *individual* level. Individuals, as digital identity subjects often keenly involve themselves in identity management to gain control over their digital identities. To this end, various personalised commercial identity management solutions like Garlik's[508] DataPatrol and Reputation Defender, and non-commercial identity management solutions like ClaimID have been developed.

---

[505] P Wood, 'Implementing Identity Management Security: An Ethical Hacker's View,' (2005) 9 Network Security, 12-15
[506] See Windley (2005) **n122**
[507] Caplan (2001) **n98**. See also D Lyon, *Identifying Citizens:ID Cards as Surveillance* (Polity Press, Cambridge 2009)
[508] <http://www.garlik.com/>

Garlik's DataPatrol[509] is an Internet based identity management service that helps businesses and individuals manage their digital identities for a fee. DataPatrol aims at monitoring and alerting an identity subject if their digital identity information – whether it is in the form of a user name, financial data, or email addresses, is at risk or has been compromised.

Reputation Defender,[510] claiming to be the "world's first comprehensive online reputation management and privacy company," aims at seeking information available about digital identity subjects on the Internet and intimating them of the same, providing them with assistance to destroy and correct it if required and helping digital identity subjects construct their digital profiles. Its other products are: MyReputation, MyChild, MyEdge and MyPrivacy.

ClaimID[511] is a free identity management tool for individuals to manage their online identities. It provides them with an OpenID to log into different websites without having to create new user names or passwords for each of them. The digital identity subject outlines to ClaimID all its online identities, which then enables the identity subject to have an easy means of proving ownership of these identities.[512] The digital identity subject's profile uses Microformats[513] like the hCard.[514] ClaimId also aims at helping individuals manage their online identities by making cached information available to them in case the original version of the website disappears.

Digital identity management, whatever its form, represents a form of empowerment. In the context of *organisational* digital identity management, it seeks to empower the organisation; in *governance*, it seeks to empower the State in the performance of its

[509] <http://www.garlik.com/products.php>
[510] <http://www.reputationdefender.com/company>
[511] <http://claimid.com/>
[512] This is highly debatable as the possession of online identities does not necessarily denote an ownership of identities, as demonstrated in **Ch 2 (2.5.6)**
[513] Microformats are "a set of simple, open data formats built upon existing and widely adopted standards." See <http://microformats.org/>
[514] An hCard is "a simple, open, distributed format for representing people, companies, organizations, and places, using a 1:1 representation of vCard (RFC2426) properties and values in semantic HTML or XHTML." <http://microformats.org/wiki/hcard>

functions and when used by *individuals* it seeks to empower them in the control of their digital identities.

In addition to the above classification (*Organisational, Governance and Individual*), there are other classifications of identity management systems.[515] Prominent is the three tier classification proposed by Bauer, Meints and Hansen,[516] which classifies identity management systems into three types:

> **Type 1**: Systems for account management, implementing authentication, authorisation, and accounting[517]
> **Type 2**: Systems for profiling of user data by an organisation, e.g. detailed log files or data warehouses which support e.g., personalised services or the analysis of customer behaviour[518]
> **Type 3**: Systems for user-controlled context-dependent role and pseudonym management.[519]

Type 1 systems are account management systems, used within an organisation largely for account and access administration for computers and network services (e.g. the Windows-NT-Domain-concept by Microsoft, NIS by SUN). This is similar to the *organisational* classification of digital identity management and includes identity management carried out by big identity and service providers. Type 2 systems involve profiling techniques. While the examples in the classification by Bauer, Meints and Hansen are primarily business related, other examples of Type 2 systems are those used by States in governance - at border control, in the determination of rights or entitlements to services, or systems used in the criminal

---

[515] Yi Qian, D Tipper, P Krishnamurthy, J Joshi, *Information Assurance: Dependability and Security in Networked Systems* (Morgan Kaufmann Publishers, San Francisco 2007), 72 (classification made in terms of identity provider centric frameworks and user centric frameworks); DGW Birch, 'The Identity Vision,' in DGW Birch (ed), *Digital Identity Management: Perspectives on the Technological, Business and Social Implications* (Gower, Hampshire 2007), 4-5 (classified as technology tools).

[516] M Bauer, M Meints and Hansen (eds.), 'FIDIS Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems,' Frankfurt a.M., (2005),<http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf>

[517] *Citing* <http://infosecuritymag.techtarget.com/2002/apr/cover_casestudy.shtml>, <http://www.oracle.com/technology/products/id_mgmt/index.html> and <http://www3.ca.com/Solutions/ProductFamily.asp?ID=4839>

[518] *Citing* <http://www.lumeria.com/what.shtml>, <http://www.epic.ca/TechnologyDay/October05_2004/MoreInformation/Presentations/RandallBartsch%20-%20Identity%20Mgmt.pdf>

[519] *Citing* ICPP, ULD and SNG, *Identity Management Systems (IMS): Identification and Comparison Study* (September 2003) <http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMSStudy.pdf>

justice system. Type 3 systems are systems characterised by user control. They are decentralised, user and client-orientated, where the data managed are largely personal data and of which privacy functions as the unique selling point.[520]

Thus, digital identity management is about controlling digital identity, in different manners, by different entities and at various levels that could be exclusive or mutually co-existing.

4.5. Models of digital identity management

Based on their development and nature, digital identity management systems can be classified into three models: centralised identity systems, federated identity systems and user centric identity systems.

4.5.1. Centralised

Centralised identity systems were the initial identity management market offering to deal with the problem of multiple identities and promote Internet security. A centralised identity system is one where a central identity management system provider "acts as a single gateway for the user's management of identities."[521] Centralised identity management systems because of their centralised nature are easy to administer, convenient and affordable as compared to other options.

How centralised identity management works is simple: one entity acts as the identity provider, authenticates identity subjects and issues identity tokens which can then be used across pre-authorised organisations.[522] Going back to our earlier discussion, digital certificates are a key example of centralised identity management in action.

Microsoft Passport or Windows Live ID[523] is an example. This system was a credential system that permitted digital identity subjects to log in to multiple sites

[520] Bauer (2005) **n516,** 14
[521] ICPP (2003) **n519**
[522] R Dhamija and L Dusseault, 'The Seven Flaws of Identity Management: Usability and Security Challenges' (2008) 6 (2) IEEE Security & Privacy, 24-29
[523] <https://accountservices.passport.net/ppnetworkhome.srf?vv=900&mkt=EN-GB&lc=2057>

and services on the Microsoft Passport Network with a single sign on. A Passport user account comprised of several elements like: the PUID,[524] a unique 64-bit number encrypted and authenticated on request; user profile containing mandatory information like the user's e-mail address, telephone number and optional information like user's name, demographic information and credentials (password and pin, security questions). The advantages of this system were that it eliminated the need for a user to log in multiple times and secured his digital identity in one place - on the Passport database. In the process of this management of a user's identity, Passport used cookies to facilitate the conduct of its identity management operations.[525]

Passport came under severe criticism.[526] The first ground was that Passport was inadequately secured and susceptible to compromise.[527] This was compounded by the fact that Passport employed user selected passwords as a security measure.[528] Other criticisms related to its centralised and anti-privacy nature.[529]

The US FTC launched an investigation into Passport, taking cognizance of a complaint by several consumer organisations headed by EPIC.[530] Some of the charges were that Microsoft, in its Passport services, had falsely promised "reasonable and appropriate measures" to safeguard "the privacy and confidentiality of consumers' personal information" and stated that it did not collect any personally

[524] Passport User ID
[525] See 'Windows Live ID,' Microsoft Passport Network Privacy Statement, (April 2005) <https://accountservices.passport.net/PPPrivacyStatement.srf#1>
[526] R Oppliger, 'Microsoft .NET Passport and Identity Management,' (2004) 9 (1) Information Security Technical Report, 26-34; M Slemko, 'Microsoft Passport to Trouble' (5 November 2001) <http://www.znep.com/~marcs/passport/>; D Becker, 'Passport to Nowhere?' *CNET News.com* (23 March 2004); DP Kormann and AD Rubin, 'Risks of the Passport Single Signon Protocol,' (2000) 33 Computer Networks, 51–58
[527] James Snell, Doug Tidwell and Pavel Kulchenko, *Programming Web Services with SOAP* (O'Reilly, USA 2001), 155
[528] Robert Lemos, 'Password Flaw Cracks Passport Security,' *CNET News.com* (8 May 2003)
[529] See Ann Cavoukian and Tyler Hamilton, *The Privacy Payoff: How Successful Businesses Build Consumer Trust* (McGraw Hill, Canada 2002), 190
[530] *In the Matter of Microsoft Corp.,* FTC Docket No. C-4069 (20 Dec. 2002)

identifiable information, when it did.[531] Even the EU launched a formal investigation into Passport for data protection breaches.[532]

Another example of centralised identity management is the Kerberos Network Authentication Service. [533] Kerberos provides a "means of verifying the identities of principals, (e.g. a workstation user or a network server) on an open (unprotected) network."[534] Using conventional cryptography, it works as a trusted third party authentication service. Kerberos (version 5) is implemented in Windows 2000 and 2003 as the default authentication standard.[535] Though Kerberos has its pros, it also has its cons. Key among these are implementation and compatibility problems, trust and risk issues, and mostly, that it is an all or nothing solution.[536]

Despite their advantages (ease, convenience and affordability), centralised identity management systems, as demonstrated, have significant problems. They are hierarchical, prone to implementation and governance issues,[537] vulnerable to targeted scams and compromises, subject to political or commercial abuse and susceptible to system failures.[538] These are but some of contributory factors that led to their rejection and failure.

4.5.2. Federated

Federated identity systems (also called circles of trust)[539] developed in response to the shortcomings of centralised identity management systems. According to Maler and Reed, federated identity management "is a set of technologies and processes that let computer systems dynamically distribute identity information and delegate

[531] FTC, 'Microsoft Settles FTC Charges Alleging False Security and Privacy Promises,' (8 Aug 2002) <http://www.ftc.gov/opa/2002/08/microsoft.shtm>
[532] Reuters, 'EU: MS Passport Is Under Investigation,' (2002) <http://zdnet.com.com/2100-1104-934916.html> ; Seagrumn Smith, 'Microsoft and the European Union Face Off Over Internet Privacy Concerns,' (2002), Duke L & Tech Rev 0014
[533] J Kohl and B Clifford Neuman, 'The Kerberos Network Authentication Service (Version 5),' Internet Request for Comments RFC-1510, (Sept 1993)
[534] ibid
[535] <http://technet.microsoft.com/en-us/library/cc784935(WS.10).aspx>
[536] Red Hat Inc, Kerberos, <http://www.centos.org/docs/5/html/Deployment_Guide-en-US/ch-kerberos.html>
[537] Windley (2005) **n122,** 119
[538] Windley, (2005) **n122,** 120
[539] Terminology made popular by the Liberty Alliance.

identity tasks across security domains."[540] Simply stated, federation is a reference to "the agreements, standards, and technologies that make identity and entitlements portable across autonomous domains."[541]

In a federated identity system, different entities work within the "umbrella of common policies and mechanisms across disparate local identity systems" in the identity management process.[542] Federation is beneficial as it enables entities and organisations to control, manage and share multiple digital identities effectively, efficiently and in cost effective manner.[543] In the federated model of identity management systems, there is no single entity with overall control. These systems support digital identity across multiple providers in a distributed and piece meal fashion. OASIS Security Assertion Markup Language (OASIS SAML) and Liberty Alliance are standards for identity federation, while Shibboleth represents an open source implementation of the federated model of identity management.

OASIS SAML, per Cantor and others,

> defines the syntax and processing semantics of assertions made about a subject by a system entity. In the course of making, or relying upon such assertions, SAML system entities may use other protocols to communicate either regarding an assertion itself, or the subject of an assertion. This specification defines both the structure of SAML assertions, and an associated set of protocols, in addition to the processing rules involved in managing a SAML system.[544]

The Liberty Alliance was set up in 2001 as a global identity consortium between around thirty organisations to develop "open technical, business and privacy standards for federated identity management."[545] It released the Liberty Federation in 2002, Liberty Web Services in 2003 and ID-SAFE (Identity Strong Authentication

---

[540] E Maler and D Reed, 'The Venn of Identity: Options and Issues in Federated Identity Management,' (2008) 6 (2) Security and Privacy: IEEE in Security & Privacy, 16-23
[541] As defined by the Burton Group. See 'Primer on Federated Identity,' <http://www.sourceid.org/content/primer.cfm>
[542] Windley (2005) **n122,** 122
[543] D Smith, 'The Challenge of Federated Identity Management,' (2008) 4 Network Security, 7-9
[544] S Cantor, J Kemp, R Philpott and E Maler (eds), 'OASIS: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0,' OASIS Standard, Security Services Technical Committee (15 March 2005), <http://docs.oasis-open.org/security/saml/v2.0/>
[545] <http://www.projectliberty.org/>

Framework, stated to be the "industry's first open framework for deploying and managing interoperable strong authentication.")[546]

Liberty Web Services is made up of the Identity Web Services Framework (ID-WSF) and the Identity Service Interface Specifications (ID-SIS), both of which jointly enable identity-based services.[547] The ID-WSF in its operation, "builds on many existing standards for networking and distributed computing, and adds specialized capabilities for handling identity-related information." [548] The following diagram illustrates the Liberty Web Services Architecture:[549]

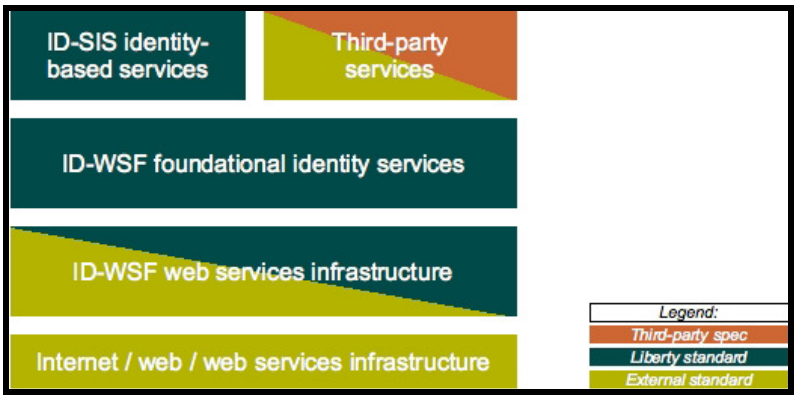

Fig 5: The Liberty Web Services Architecture

Shibboleth[550] is a "standards based, open source software package for web single sign-on across or within organizational boundaries." It is used to facilitate single sign on access to a multiplicity of resources within an organisational network. For the developers of Shibboleth (Internet2Middleware[551] and Middleware Architecture Committee for Education),[552] the privacy of the digital identity subject was a key

---

[546] <http://www.projectliberty.org/>
[547] C Cahill and ors, 'Liberty Alliance Web Services Framework: A Technical Overview,' Vers.1.0, (14 Feb 2008) <http://www.projectliberty.org/liberty/content/download/4120/27687/file/idwsf-intro-v1.0.pdf>
[548] ibid
[549] Cahill (2008) **n547**, 4
[550] <http://shibboleth.Internet2.edu/>
[551] Internet2 is a US based non-profit advanced networking consortium comprising more than 200 US universities collaborating with 70 leading corporations, 45 government agencies, laboratories and other higher learning institutions and 50 international partner organizations. See <http://www.Internet2.edu/about/>
[552] MACE comprises of a group of US and international higher-education IT architects "formed to investigate the creation of a national interoperable identity and access management infra-structure for the U.S. research and education community that would fit into a global context." <http://www.Internet2.edu/middleware/about.html>

consideration. In fact, it was one of the primary goals of the design of the technology.[553]

A Shibboleth transaction occurs as follows:

> Amy wants to access the University of Edinburgh Legal Research Resources. In her attempt to do so she is directed to the WAYF federation, where she selects her home institution (her identity provider) from WAYF's list of authorised identity providers. Her identity provider authenticates her, which generates a handle or session identifier for Amy's session that is sent to the service provider. The service provider checks this handle out with the identity provider and accordingly provides or denies Amy access to the resources.

While Shibboleth has its merits (i.e. it facilitates inter-organisational single sign on access), it also has its downsides, as outlined by Harrison and Bramhall:

(i) The individual can only transfer attributes recorded by the organisation which hosts his Shibboleth account, rather than by any third party;
(ii) The individual cannot choose which organisation hosts his Shibboleth account and
(iii) The scheme lacks a business model that would allow different service providers to share the costs of secure authentication and permissioned attribute transfer.[554]

There are three types of federated identity management systems per Windley: *ad hoc*, *hub and spoke* and *identity networks*.[555] *Ad hoc* systems support identity relationships on an ad hoc basis. *Hub and spoke* systems are represented by different entities being clustered around a rule making strong entity. *Identity networks* (examples cited are Ping Identity and SXIP) are independent entities which primarily focus on the "technical and administrative aspects of identity federation."[556]

Ping Identity[557] provides Internet Identity Security and Single Sign-On (SSO)[558] solutions like PingFederate and PingConnect, which mostly use federated identity

---

[553] <http://www.Internet2.edu/pubs/shibboleth-infosheet.pdf>
[554] J Harrison and P Bramhall, 'New Approaches to Identity Management and Privacy: A Guide Prepared for the Information Commissioner,' (December 2007) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/edentity_hp_idm_paper_for_web.pdf>
[555] Windley (2005) **n122,** 118-132
[556] Windley (2005) **n122,** 128
[557] <http://www.pingidentity.com/>

standards.[559] PingFederate functions as a SSO Service for multiple web applications.[560] PingConnect is a SaaS (Software as a Service) SSO service aimed at working with SAML (or WS-Fed)-enabled SaaS applications.[561]

SXIP,[562] founded by Dick Hardt in 2003, aims at making web interactions more simple and convenient through the development of a "secure and open identity architecture that enables individuals to easily manage their online digital identities."[563] SXIP's identity solution is Sxipper,[564] a free add-on for Firefox which enables digital identity subjects to log in securely to different websites. Sxipper tracks multiple user ids, passwords and personal data shared on the Web.

Another example of a federated identity management solution is VeriSign® Identity Protection (VIP) services made up of the VIP Authentication Service and the Fraud Detection Service inter alia.[565] VIP Services work on the basis of two-factor authentication, self-learning fraud detection and validation infrastructure. The VIP Authentication Service, particularly functions in the following manner: it takes 'something' the digital identity subject 'knows' (like a user name, password) and unifies it with 'something' the digital identity subject 'has' (e.g. a smartcard, token, or mobile phone) and validates it. The VIP Fraud Detection Service processes transactions to determine fraud risks based on rules and self-learning. If a risk element is found, then higher levels of authentication are imposed.[566] Investigations can then be quickly carried out and resolved.

---

[558] SSO is a "mechanism whereby a single action of user authentication and authorisation can permit a user to access all computers and systems where he has access permission, without the need to enter multiple passwords." The Open Group, SSO, <http://www.opengroup.org/security/sso/>
[559] <http://www.pingidentity.com/>
[560] For further details see <http://www.pingidentity.com/our-solutions/pingfederate.cfm>
[561] For further details see <http://www.pingidentity.com/our-solutions/pingconnect.cfm>
[562] Expanded, Simple eXtensible Identity Protocol
[563] <http://www.sxip.com/background>
[564] <http://www.sxipper.com/>
[565] <http://www.verisign.co.uk/authentication/consumer-authentication/identity-protection/index.html>
[566] <http://www.verisign.co.uk/authentication/consumer-authentication/vip-fraud-detection-services/index.html>

Federated identity systems have their own set of problems.[567] They frequently are piece meal, free for all and complex to manage. They have security and control,[568] and funding and partner relationship issues between the entities.[569] They are also beset with trust complexities[570] and unsolved liability issues.[571] Problems are also evident in regards to the transfer of data outside clusters (or established circles) and have been criticised for being too abstract.[572]

4.5.3. User centric

The failure of centralised and federated identity management systems to meet expectations of industry and digital identity subjects in the digitally advanced West led to the development of user-centric identity management (also called Identity 2.0).[573] This form of identity management aims at giving digital identity subjects (in this form of identity management generally referred to as users) superior control over their digital identities, as compared to the previous two models.

User-centric forms of identity management have two key features, according to Hansen: first, its ability to make identity attributes flows more explicit and give users more 'notice and choice' over their digital identities and second, its ability to be privacy enhancing through enabling data minimisation and promoting data unlinkability.[574] The first instance, Hansen reckons, is a reflection of the right to informational self-determination.[575] Here is evident the embedding and connection of

[567] Windley (2005) **n122,** 126-127, 132
[568] A point also made by Abhilasha Bhargav-Spantzel, AC Squicciarini & E Bertino, 'Establishing and Protecting Digital Identity in Federation Systems,' CERIAS Tech Report 2007-18, <https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2007-18.pdf>
[569] Windley (2005) **n122,** 132
[570] Jøsang (2005) **n503**
[571] Windley (2005) **n122,** 132
[572] Dr Earl R Smith II, 'Can't We Simplify Digital Identity,' Guest Article, *The Federal Circle* (26 August 2010)
[573] The main role of Identity 2.0 is stated to be "to provide users with full control over their virtual identities." Vacca (2009), **n122,** 278
[574] M Hansen, 'Marrying Transparency Tools With User-Controlled Identity Management,' in S Fischer-Hubner and ors, (eds), *The Future of Identity in the Information Society*, IFIP 262 (Springer, Boston 2008), 199-220, 202
[575] The right to informational self determination here taken as referring to "…the capacity of the individual to determine in principle the disclosure and use of his/her personal data" as defined in the well known *Volkszählungsurteil* decision by the German Federal Constitutional Court (*Bundesverfassungsgericht*) in 1983, BVerfGe 65, 1. Text at <http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm>. The right is defined by Rouvroy and Poullet as "an individual's control over the data and information produced about him is a (necessary but insufficient) pre-condition for him to live an existence that may be self-determined." Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy,' in Serge Gutwirth and ors (eds), *Reinventing Data Protection* (Springer, Berlin 2009), 45-76, 51

a European legal value into the technology of identity management. User-centric identity management is also seen as an indispensable tool for privacy protection.[576]

The user-centric model is manifest in the Laws of Identity, which state:[577]

1. **User Control and Consent:** Technical identity systems must only reveal information identifying a user with the user's consent.
2. **Minimal Disclosure for a Constrained Use:** The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution.
3. **Justifiable Parties:** Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
4. **Directed Identity:** A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles
5. **Pluralism of Operators and Technologies:** A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.
6. **Human Integration:** The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks
7. **Consistent Experience across Contexts:** The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

All the principles of the Laws seek to fulfil the right of a digital identity subject to its digital identity. They aim at giving the digital identity subject control over its digital identity through setting limits on the amount of personal identity information given out, making disclosures subject to consent, offering choices in identity services and facilitating informed and rational decisions by identity subjects about their digital identities.

Many of the tenets of the Laws of Identity find basis in Western data protection law like the Personal Data Principles embodied in the OECD Guidelines on the

[576] RE Leenes, 'User-Centric Identity Management As An Indispensable Tool For Privacy Protection,' (2008) 2 (4) IJIPM, 345 - 371

[577] Cameron (2005) **n131;** The Laws of Identity, since their original enunciation, were refined to a shorter version which is available at <http://www.identityblog.com/?p=1007>

Protection of Privacy and Transborder Flows of Personal Data,[578] the fundamental right of an individual in the EU to their personal data as embodied in Article 8 of the Charter of Fundamental Rights of the European Union[579] and the EU Data Protection Directive.

The OECD Guidelines aim to help protect privacy and individual liberties in the processing of private and public sectors. In Part 2, they contain basic principles in respect of data protection like collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. In many respects the Laws of Identity embody these principles. For example, the requirement to reveal information only with consent (relative to collection limitation principle), minimal disclosure (use limitation principle), justifiable parties (security safeguards) and human integration (individual participation principle).

The EU Data Protection Directive embodies the fundamental principles required to be followed in the processing of personal data. These principles are reflected in the Laws of Identity. For instance, the fair and lawful processing of data[580] (embodied in principle 1 of the Laws of Identity), purpose limitation[581] (principles 2 and 4 of the Laws of Identity), data adequacy[582] (principle 2 of the Laws of Identity), accuracy of data[583] and time limitation[584] (principle 2 of the Laws of Identity).

The Laws of Identity, though representing a useful technical contribution to furthering the user-centric model of identity management, have been subject to criticism. Donley analyses each principle (of the shortened version) in part and raises

[578] OECD Doc C58 Final (1 October 1981)
[579] The Article states that everyone has the right to the protection of personal data concerning him or her; that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law and that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. It also states that compliance with these rules shall be subject to control by an independent authority.
[580] Art 6 (1) (a)
[581] Art 6 (1) (b)
[582] Art 6 (1) (c)
[583] Art 6 (1) (d)
[584] Art 6 (1) (d)

some serious issues.[585] For instance, the difficulty of achieving user control (first principle) especially in the online context given free content and the drive to collect and share increasing amounts of information. He also finds the third principle (no automatic linkability and no single identifiers) hard to accomplish. The Laws are also not grounded in the reality of how people use and relate to digital identities and associative technologies and might lay digital identity subjects open to new threats and dangers.[586] This is particularly concerning given our analysis in Chapter 3.

Windows CardSpace implements the Laws of Identity and the user centric paradigm of identity management. Other examples of user centric identity management initiatives are: OpenId, IBM's Idemix, Higgins, and PRIME.

4.5.3.1.Windows CardSpace

Windows CardSpace (or InfoCards) is part of .NET Framework 3.0 and is available with Windows Vista, Windows XP, Windows Server 2003 and Windows 7. Windows CardSpace is an identity cards infrastructure, similar to those supporting passports or credit cards, aimed at helping users prove their identity in their online transactions.

InfoCards are connected to identity information issued by an identity provider (entity or organisation like a bank, employer, government or even the digital identity subjects themselves). The advantages of the InfoCards are cited as being: flexibility, consistency in user experience, greater security (as compared to passwords), and a greater ability to accommodate identity queries and requests.[587] These InfoCards implement the U-Prove[588] technology which is hailed as being a good example of 'minimal disclosure' technology. Minimal disclosure technology facilitates the protection of the privacy and anonymity of the digital identity subject and functions

[585] C Donley, 'Revisiting the Laws of Identity' Oracle, (18 August 2008) <http://blogs.oracle.com/clayton/2008/08/revisiting_the_laws_of_identit.html>
[586] ibid
[587] <http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx>
[588] Created by S Brands, <http://www.credentica.com/u-prove_sdk.html>. Acquired by Microsoft from Credentica.

on the basis of minimal and selective disclosure of identity information, unlinkability and non-transferability.[589]

4.5.3.2.OpenId

OpenId is an open source and decentralised identity management standard for user authentication and access control that allows digital identity subjects to log into and access different services with an existing digital identity. It thus eliminates the need for multiple authentications.

How OpenId works is simple: A digital identity subject creates an OpenId account with an OpenId provider choosing a username, password and authenticating with a Captcha.[590] Once the OpenId account is created, the digital identity subject can log in to any website that permits an OpenId login. The digital identity subject enters OpenId login into the websites log in form. The website then directs the digital identity subject to the OpenId provider to log in using the OpenId username and password. The digital identity subject then indicates to OpenId that the website requesting the information can use its identity. Once this is confirmed, the process is complete and the digital identity subject is authenticated at the website without having to create a separate identity to log in. A person may have any number of OpenIDs.[591]

---

[589] See Brands (2000) **n481**, 32, 91. Microsoft seems to prefer the use of the terms 'unlinkability' and 'selective disclosure' rather than 'anonymity and pseudonymity' though these seem to be the underlying values sought to be promoted.

[590] A Captcha (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is "a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot." The term was coined by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University in 2000. <http://www.captcha.net/>

[591] For a full primer on OpenId see screen cast by S Willison, 'How to Use OpenId,' (22 December 2006), <http://www.youtube.com/watch?v=Vq0R1Y1A2rE&feature=player_embedded>

4.5.3.3.IBM's Idemix

IBM's Idemix,[592] developed by researchers at IBM's Zurich Research Laboratory in Rüschlikon, Switzerland, is based on the concept of 'data parsimony' which supports the view that "personal data is best protected if not revealed at all, i.e., if the amount of data revealed is kept to a minimum." This technology endeavours to protect individual privacy through concealing personal information.

The Idemix system is an anonymous credential system, as outlined by Camenisch and Herreweghen,[593] based on the protocols developed by Camenisch and Lysyanskaya.[594] Per Camenisch and Herreweghen,[595] the central feature of Idemix is the NymSystem package[596] which implements the UserNymSystem, OrgNymSystem and De-AnOrgNymSystem components all of which proffer "functionality related to the specific cryptographic operations executed by the different entities, as well as methods to create a new instance of the entity by generating cryptographic key material (user master secret, organization's public/private key pair, de-anonymising organization's public/private encryption key pair)."[597]

4.5.3.4.Higgins

Higgins[598] is an Eclipse Project[599] open source identity software framework,[600] designed through collaboration between developers from Novell, Azigo, IBM,

---

[592] IBM Research, 'IDEMIX (Identity mixing),'<http://www.zurich.ibm.com/pri/projects/idemix.html>
[593] Camenisch (2002) **n426**
[594] J Camenisch & A Lysyanskaya, 'Efficient Non-Transferable Anonymous Multi-Show Credential System With Optional Anonymity Revocation,' in B Pfitzmann (ed), *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology* (Springer Verlag, London 2001), 93–118
[595] Camenisch (2002) **n426**
[596] For full details, see M Bove, *Key Management, Setup and Implementation of an Anonymous Credential System* (Master's Thesis, 2001).
[597] Camenisch (2002) **n426**
[598] <http://www.eclipse.org/higgins/>
[599] The Eclipse Project was created by IBM in November 2001 and the Eclipse Foundation in January 2004 as an independent not-for-profit corporation. For list of members see <http://www.eclipse.org/membership/showAllMembers.php>
[600] Higgins is a software infrastructure (not protocol) that works with most digital identity protocols including WS-Trust, OpenID, SAML, XDI, LDAP, etc.

Meristic, Harvard Law Lab and Serena, and previously included people from the Intertechnogroup, NCSU, OCLC and Freeshell.[601] The aims of Higgins are: providing an identity and security layer for the Internet, giving users more control over their digital identities,[602] enhancing privacy[603] and security, providing a simple and consistent user experience,[604] identity data integration, facilitating cross-platform identity selectors and enabling interoperability.[605] Higgins enables users through an add-on browser (or selector) to log into websites and control the dissemination of their personal information.

4.5.3.5.PRIME

The PRIME project, funded by the EU's Sixth Framework Programme and the Swiss Federal Office for Education and Science, concentrated on the development of a working prototype of a privacy-enhancing identity management system, with the collaboration of people from industry, academia and research.[606]

The PRIME[607] architecture on which the PRIME identity management system is based is another prolific example of a user centric system. At its heart, is the vision to protect individual privacy.[608] This comes out acutely in its apparent and persistent focus on privacy protection, both in how its goals are expressed and the nature of the system itself.[609] The PRIME system follows the following principles:[610]

1. Design must start from maximum privacy.
2. Explicit privacy rules govern system usage.

---

[601] <http://www.eclipse.org/higgins/team-leaders.php>
[602] <http://www.eclipse.org/higgins/faq.php#new-update-site5a>; Also see Higgins Charter, point 2 at <http://www.eclipse.org/higgins/higgins-charter.php>
[603] <http://www.eclipse.org/projects/project_summary.php?projectid=technology.higgins>
[604] ibid
[605] Higgins Overview 2009, <https://dev.eclipse.org/svnroot/technology/org.eclipse.higgins/trunk/doc/org.eclipse.higgins.doc/Higgins-Overview-2009.pdf>
[606] The duration of the PRIME project was March 2004-February 2008.
[607] See <https://www.prime-project.eu/>
[608] D Sommer, M Casassa Mont, S Pearson, 'PRIME Architecture V3,' Deliverable D14.2.d, (9 July 2008) <https://www.prime-project.eu/prime_products/reports/arch/pub_del_D14.2.d_ec_WP14.2_v3_Final.pdf>
[609] See Sommer (2008), § 9.2.2 (Privacy Obligation Aspects), 45
[610] PRIME General Public Tutorial, Vers. 2 (May 2008) <http://blues.inf.tu-dresden.de/prime/GPTv2/englisch/PRIME_nm.htm>

3. Privacy rules must be enforced, not just stated.
4. Privacy enforcement must be trustworthy.
5. Users need easy and intuitive abstractions of privacy.
6. Privacy needs an integrated approach.
7. Privacy must be integrated with applications.

The PRIME system is to provide the following functions: administration of digital partial identities, event logging (history), negotiation of privacy policies, support of privacy obligations through appropriate tools and mechanisms, identity and privacy centred decision making support, anonymous communication, self-assessment of identity services and platforms.[611] More technically, the PRIME system

> is a data and metadata processing system supporting entities in making decisions by suggesting choices and in using cryptographic methods to support their statements and validate those of others. In order to suggest choices rules (called policies) and knowledge containing past and present facts (called decision context) need to be considered.[612]

The PRIME system comprises of two segments: the service-side module and the user-side module (also called the PRIME Middleware, which runs on the identity subject's computer and facilitates PRIME enabled applications). The Middleware features a PRIME management console which gives the identity subject/user the power to control (most importantly, this means to withhold the disclosure of) its digital identity. The service side of the PRIME system mainly provides access control functionalities and handles trust and policy negotiations, as well as data disclosure protocols and privacy obligations. These are necessary functionalities for the service provider to ensure that users' decisions concerning their privacy preferences are respected.

The PRIME project also manifests in PrimeLife, which carries forth the work of PRIME.[613] PrimeLife is even more privacy stringent than the PRIME project. This is evident in its main objective of enabling sustainable privacy and identity management to future networks and services and sub-objectives of understanding

[611] ibid
[612] PRIME Advanced Tutorial, Vers. 3 (May 2008) <http://blues.inf.tu-dresden.de/prime/Tutorial_V2/DevTut.html>
[613] <http://www.primelife.eu/>

privacy-enhancing identity management for life, developing web privacy, and expanding and propagating tools for privacy friendly identity management.[614]

User centric models of identity management have their problems. There are implementation issues as they require change in organisational and business identity set ups and their adoption has been relatively slow.[615]

Coming out loud and clear in the proposals and development of user centric models of identity management is the vision and need to enhance user control and the achieve maximum privacy. Most of the user centric models highlighted above seek to embody this vision in their design and implementation. But, as cautioned before, this is a vision that is highly Western centric, and highly problematic given local difference.

4.6. Allied developments: Privacy by Design

'Privacy by design,' was developed by the Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian in the nineties, and refers to

> the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices (FIPs)[616] into the design, operation and management of information processing technologies and systems.[617]

Privacy by design developed in the West and embodies the expectations and needs of the digitally advanced societies that place high premiums on the value of privacy of

---

[614] <http://www.primelife.eu/about/factsheet>
[615] Harrison (2007) **n554**
[616] The FIPs are: Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security and Enforcement/Redress. They were initially developed in the US where they were detailed in the US Department of Health, Education and Welfare's 1973 seminal report entitled 'Records, Computers and the Rights of Citizens,' (1973). See also: The Privacy Protection Study Commission, 'Personal Privacy in an Information Society,' Report (July 1977) <http://epic.org/privacy/ppsc1977report/>; Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, 'Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information' (6 June 1995) <http://aspe.hhs.gov/datacncl/niiprivp.htm>; US Dept. of Commerce, 'Privacy and the NII: Safeguarding Telecommunications-Related Personal Information,' (October 1995) <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>; CSA, *Model Code for the Protection of Personal Information: A National Standard of Canada* (CSA, Etobicoke 1996)
[617] Ann Cavoukian, *Privacy by Design… Take the Challenge*, (Jan 2009), iv, <http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf>

personal information. This approach envisages privacy as the starting point and default in digital identity management[618] through the following measures:[619]

1. Acknowledgement of the need to address privacy concerns
2. Application of the basic principles expressing the universal spheres of privacy protection
3. An early alleviation of privacy concerns in the development of any technologies
4. Qualified privacy leadership and/or professional input; and
5. Adoption and integration of PETs.

Privacy by design speaks of applying the basic principles expressing universal spheres of privacy protection. But, there is no such thing as a 'universal sphere of privacy' or privacy protection, as demonstrated in Chapter 3,[620] and will further substantiated in Chapters 5[621] and 6.[622]

Privacy by design was applied in relation to Facebook in 2009. Facebook changed its privacy and security policies to comply with Canada's privacy law after discussion with the Canadian Office of the Privacy Commissioner (OPC) in line with their recommendations.[623] Here, the need to address privacy concerns, under the assumption that there are universal spheres of privacy protection, led to a change in the design of a global identity platform with 250 million global digital identity subjects. Action was initiated on the basis of Canadian privacy law that had an effect on digital identity subjects who may or may not have similar expectations, privacy needs or subscribe to the privacy or personal data protection principles as do Canadians.

Thus, privacy by design in the manner it currently manifests fails to take into account the simultaneous global and local nature of digital identity and the local contexts of digital identity subjects.

---

[618] Much like the PRIME system.
[619] ibid, 3
[620] **3.2.2.1**
[621] **5.2.2.1**
[622] **6.3.1**
[623] M Hartley, 'Facebook to Tweak Its Privacy, Security Policies To Meet Canadian Law,' *Financial Post* (17 August 2009) <http://www.financialpost.com/news-sectors/technology/story.html?id=1901523>

4.7. Evaluation of Digital Identity Management

This part now analyses whether digital identity management measures up as an effective regulator of digital identity. More importantly it also analyses whether digital identity management as currently packaged takes into account the local context of digital identity. To this effect, this part first outlines some of the general and universal problems of digital identity management;[624] then, it specifically shows how digital identity management fails to take into account the local context of digital identity.[625]

4.7.1. Mirroring of paper based systems

One of the key criticisms of digital identity management systems is that they mirror paper based identity management systems. This was a problem particularly highlighted by Jean Camp who states that, "paper-based centuries-old concepts of identity are being stapled into the digital age."[626] Jean Camp differentiates between paper and digital identity and believes that papers are a different form of technology, capable of being "physical self-confirming," less prone to transactional histories and with controllable accessibility and dissemination possibilities.[627] Digital identity management systems, in their mirroring of paper based identity systems, leave digital identity subjects prone to hazards and risks like unmanageable linkage, traceability and permanence. These risks and hazards are far more advanced and problematic than the risks of paper based systems.

4.7.2. Tools of surveillance

Digital identity management systems have another inherent problematic aspect; they can function as tools of surveillance.[628] The administration of identity inevitably also

---

[624] **4.7.1 - 4.7.5**
[625] **4.7.6, 4.7.7**
[626] L Jean Camp, 'Digital Identity,' (2004) 23 (3) IEEE Technology and Society Magazine, 34-41, 39
[627] ibid, 40
[628] Michael Freeman, 'Counterterrorism and Privacy: The Changing Landscape of Surveillance and Civil Liberties,' in Lee Freeman and Graham Peace (eds), *Information Ethics: Privacy and Intellectual Property* (Information Science Publishing, Hershey 2004), 163-179; O Gandy, 'The Surveillance Society: Information Technology and Bureaucratic Social Control,'(1989) 39 (3) Journal of Communication, 61-76

results in pinning down and locating digital identities in the context of time and space; creating logs of activity from which behavioural patterns can be gauged. Identity management creates trails of how and when digital identities were created, what they were used for, whether they were rejected, why they were rejected, the number of times the identity was used as also where it was used.[629]

Identity management systems have the propensity to double up as individual or mass surveillance systems.[630] This is particularly evident in the case of ID cards, national identity systems, border management systems and even online identity management tools.

The administration and control of identity through ID cards that are linked to databases creates immense opportunities for surveillance of the digital identity subject, as highlighted by Lyon.[631] Such surveillance, Lyon states, "is typically centred on data from the human body, is automated, connected with control, especially access control and aims at universal coverage within specific jurisdictions."[632]

The immense potential of identity management systems to function as surveillance mechanisms is also illustrated by identity management systems used at borders by immigration authorities to establish and authenticate identity on entry and departure from a country.[633] For instance, the use of facial recognition, iris scanning and fingerprinting.

The surveillance potential of identity management systems is also evident online in the context of the Passport and SXIP examples. Passport facilitated surveillance of

---

[629] CJ Bennett, 'Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web,' (2001) 3 (3) Ethics and Information Technology, 195-208

[630] Great Britain Parliament House of Commons Home Affairs Committee, 'A Surveillance Society?' 5th Report of Session 2007-08, Vol 2, Oral and Written Evidence, House of Commons Papers 58-II 2007-08, (TSO), 136, 273

[631] Lyon (2009) **n507**; David Lyon, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge, London 2003); David Lyon, 'Identity Cards: Social Sorting by Database,' OII Internet Issue Brief No. 3 (2004), <http://www.oii.ox.ac.uk/research/publications.cfm>

[632] Lyon (2009) **n507,** 45

[633] K Aas, 'Getting Ahead of the Game: Border Technologies and the Changing Space of Governance,' in E Zureik and MB Salter (eds) *Global Surveillance and Policing: Borders, Security, Identity* (Willan Publishing, Devon 2005), 194-214; S Graham and D Wood, 'Digitizing Surveillance: Categorization, Space, Inequality,' (2003) 23 (2) Critical Social Policy, 227-48; David Lyon, 'The Border is Everywhere: ID Cards, Surveillance and the Other,' in E Zuriek & MB Salter (eds) *Global Surveillance and Policing: Borders, Security and Identity* (Willan Publishing, Devon 2005), 66-82

digital identity subjects through use of cookies and SXIP enables surveillance through its ability to keep track of multiple user ids, passwords and personal data shared on the web.

4.7.3. Implementation and application difficulties

Digital identity management systems are also susceptible to various problems in their implementation and application. Sommer put together a comprehensive list of these:[634] point of issue failures (i.e. acceptance of erroneous credential or unauthorised identity linkages), susceptibility to management failures (e.g. failure or compromise of the database/technology validating data against presentation of credentials, failure of the database or other technology to grant privileges against credentials, failure to adequately handle and address the re-issue of lost credentials, passwords/tokens, revocation of obsolete credentials and failure of the system to perform as specified).[635]

Identity management systems may also be subject to general technology compromises like data theft, loss or cracking of passwords, token compromises, system or terminal hardware compromises, communications eavesdropping, man-in-the middle attacks and phishing.

4.7.4. Industry based regulatory uncertainty

There are also other concerns that arise in relation to identity management. While digital identity management is used to manage digital identities via digital identity management architecture (protocols, processes and systems), one source of the identity problem, the behaviour of commercial entities involved in the identity management industry is largely an unregulated free for all. This is a view supported

---

[634] P Sommer, 'Identity Management Systems: The Forensic Dimensions,' The 18th Annual FIRST Conference, Seville (June 2007) <http://www.first.org/conference/2007/papers/sommer-peter-slides.pdf>

[635] Others include emergency measures lack adequate security, compromise in the access control list or validation database, unauthorised or *ultra vires* access to and release of data, poor system protection, external breaches and corruption in management personnel.

by Gasser who questions whether "industry-controlled" self-regulatory schemes will be effective to ensure that digital identities are sufficiently protected.[636] This is because identity management practices vary from industry to industry and are subject to constant evolution.[637] The manner in which these commercial entities – private and public – conduct themselves is not transparent, open or accountable. There is much progress to be made in making digital identity management more transparent and visible to digital identity subjects and setting parameters to measure its legitimacy.

4.7.5. Presumptuousness and fallacy of user control

Digital identity management in its contemporary form, aims to provide augmented 'user control' of digital identities. User control refers to the power of the digital identity subject to determine and direct how one's digital identity, its attributes, relationships are created, constructed, maintained and decommissioned.

User control is hailed, along with privacy, as a critical factor of identity management; particularly in the user centric forms of identity management, which advocate that individuals must be placed in greater control over their identities,[638] attributes and identity relationships.[639] It is also hailed as one of the elements that determines the success or failure of an identity management system.[640]
However, user control is over rated and fraught with a number of problems.[641] Controlling digital identities may not be a primary or equal concern for all digital

---

[636] Urs Gasser, 'Identity 2.0: Privacy as Code and Policy' (9 February 2006) <http://blogs.law.harvard.edu/ugasser/2006/02/09/identity-20-privacy-as-code-and-policy/>
[637] ME Price and SG Verhulst, 'In Search of the Self: Charting the Course of Self-Regulation on the Internet in a Global Environment,' in CT Marsden (ed), *Regulating the Global Information Society* (Routledge, London 2000), 57-78, 58
[638] This message is particularly evident in the context of the UK. See Great Britain Parliament House of Lords Science and Technology Committee, *Personal Internet Security*, 5th Report of Session 2006-07, Vol. 2 Evidence, HL papers 165-II 2006-07 (TSO, 2007)
[639] A Bhargav-Spantzel, J Camenisch, T Gross and D Sommer, 'User Centricity: A Taxonomy and Open Issues,' (2007) 15 (5), J Comp Secur, 493-527.
[640] Cameron (2005) **n131**
[641] Discussed in detail in R Rodrigues, 'User Control Problems and Taking User Empowerment Further,' in V Matyáš and ors (eds), *The Future of Identity*, IFIP AICT 298 (Springer, Germany 2009), 211-225

identity subjects,[642] because individuals have a subjective relationship with digital identity. Control of digital identity can never be absolute. Also, what a digital identity subject expects and receives in the form of control might be two different things. Increased user control might also lead to increased user liability (users put in control will be expected to know and take responsibility for any acts or omissions that result in respect of their digital identity or that of others).[643]

4.7.6. Pre-occupation with privacy and data protection

Much of contemporary digital identity management, particularly solutions developed in the digitally advanced West, often begin and conclude with strong privacy and data protection arguments. The technologies examined in this Chapter demonstrate how the Western concepts of privacy and data protection have become their main stay and feature strongly in their design and orientation (as in the case of the Laws of Identity and other user centric technologies). This is highly problematic and means that digital identity management technologies and systems are not value neutral technologies,[644] containing and representing widely the privacy and data protection values of the digitally advanced West.

But, digital identity management technologies are not one continent, one country technologies. These technologies are globally rolled out and adopted. But as evidenced in the previous chapter, digital identity subjects in different countries experience digital identity divergently. Thus, the presumption made that all digital identity subjects are similarly privacy and data protection conscious, want and are

---

[642] ibid, 212

[643] Rodrigues (2009) **n641**, 217

[644] These technologies have largely developed in the West and Europe and carry within them the prevalent values and experience of these countries. Though this is not a reason to reject the validity of these technologies outright, it is relevant point to note in negotiating a regulatory future for digital identity that has both global dimensions and local relevance. Also, despite the arguments in favour of the neutrality of technology, there is a strong argument in this case that identity management technologies are non-neutral in their imbibing and carrying largely the values and experience of the digitally advanced West. This reasoning is supported in the general context of technology by Enrique Gonzalez-Manet, *The Hidden War of Information* (ABC-CLIO, Westport 1989), 53; Bonnie A Nardi and VL O'Day, *Information Ecologies: using Technology with Heart* (MIT, USA 1999), 60; SV Monsma (ed), *Responsible Technology* (WBE Publishing, Michigan 1986), 25, 31

willing and able to protect their digital identity is highly problematic if not irrelevant to societies where this is not true. Like India for example where privacy and data protection operates at entirely antithetical levels compared to the UK.

As privacy (and the expectation, need and manner of control of digital identity) is affected by local difference,[645] some identity management technologies might lose their relevance and even be subject to rejection. For instance, an identity management technology that promotes anonymity through unlinkability might be illegal in a jurisdiction where the law mandates norms of traceability and linkability. PETs and minimal disclosure technologies might be deemed socially and legally unacceptable and thus rejected. These are matters to be addressed, and not lightly dismissed, if identity management is to become universally relevant.

4.7.7. Ignorance of the local context of digital identity

Digital identity management, in contemporary form, ignores the local context of digital identity. The underlying assumption that identity management technologies are universally valid is contentious.[646] While taking all local contexts into account in the implementation of digital identity management solutions would be impossible, it must still be recognised that the dominant digital identity management solutions in current form are highly Western 'expectation, need and value oriented.' Yet, digital identity management solutions are not a one country nor one continent technology.

Digital identity management, as it currently manifests and in its embodiment of the expectations and values of the digitally advanced West does not sufficiently represent the wider world community interests specially of countries like India with different types of identity cultures and needs, and who have not been able to

[645] As determined in **Ch 3**. Further substantiated by Sandra S Petronio, *Boundaries of Privacy: Dialectics of Disclosure* (Suny, Albany 2002), 40-42; JM Gregor and T Gregor, 'Privacy: A Cultural View,' in JR Pennock and JW Chapman (eds), *Privacy Nomos XIII* (Atherton Press, NY 1971), 199-225.

[646] This assumption is manifest in the embedding of high and arbitrary privacy standards into identity management technologies.

"influence the episteme, or fundamental knowledge, upon which the regime is built."[647]

For instance in privacy centric and data protection conscious societies[648] like Europe and the UK in particular, individuals are perceived as desiring to control and manage their digital lives and identities.[649] They are seen as willing to protect their privacy and personal autonomy and taking and supporting measures to manage their identity.[650] The majority of identity management solutions aim to provide them just that,[651] as does the law.[652]

But there are global differences. In jurisdictions like India, identity management does not occur at the same level as that in the West. This is because of local difference identified in Chapter 3. Individuals bring their local contexts to digital identity, and into the need and manner of management of digital identity. Individuals who attribute a lower level of importance to privacy would be slow in the use and uptake of identity management solutions that promote this feature. Similarly individuals accustomed to their identities being part of the collective commons might not perceive the need to use identity management solutions that 'gate' their digital identities.

---

[647] DL Cogburn, 'Partners or Pawns? Implications for Developing Countries of Elite Decision-Making and Epistemic Communities in Global Information Policy on Developing Countries and Transnational Civil Society' (2005) 18 (2) Knowledge Technology and Policy, 52-82

[648] A privacy centric and data protection conscious society is one in which the protection of privacy and data ranks reasonably high in terms of desire for it. In such societies established privacy and data protection culture and norms of behaviour facilitate privacy and data protection, privacy ranks high on the public policy agenda and there is evidence of concerted efforts to protect and safeguard privacy and data. See CJ Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press, USA 2008), xi, xii

[649] Much of the digital identity and digital identity management and regulation literature based in the digitally advanced West reflects this. See Drummond Reed and Jerry Kindall, 'Digital Identity,' in Hossein Bidgoli (ed), *The Internet Encyclopedia Volume 1* (John Wiley and Sons Ltd, NY 2004), 493-504, 493; Hossein Bidgoli, *Handbook of Information Security (v. 2): Information Warfare, Social, Legal and International Issues and Security* (John Wiley and Sons Ltd, NY 2006); Roger Dean, 'Identity Management: Back to the User,' (2006) 12 Network Security, 4-7; Paul De Hert, 'Identity Management of e-ID, Privacy and Security in Europe: A Human Rights View,' (2008) 13 (2) Information Security Technical Report, 71-75; OECD (2007) **n140**, 22; Camenisch (2005) **n484**, 20-27; Cameron (2005) **n131**

[650] This has fed into the design and development of identity management solutions in the digitally advanced West. For instance, the Laws of Identity and user centric identity management.

[651] It is recognised that while people want and are able to take measures to manage their digital identities, they may choose not to do so.

[652] **Chs 5** and **6** cover this aspect.

4.8. Conclusion

This chapter appraised digital identity management - the movement and the technology, which aims at giving digital identity subjects control over their digital identities. But, digital identity management as a technical measure, while a positive development, is a limited, and by itself, incomplete tool to help individuals control their digital identity or identities, which is what it is generally sold as enabling. It is a tool that is flawed in the presumptions it makes and its ability to function as the ultimate golden or even silver bullet to safeguard digital identity of individuals.

Not just that, it is also flawed in the assumptions it makes about the universal relevance of the dominant Western values and interests it currently promotes.[653] It does not take account of local difference. This is particularly problematic given that there are divergent local contexts of digital identity and digital identity subjects as individuals from different cultures have different expectations and needs in respect of digital identity.

Therefore, we look next, to a more resilient instrument of regulating digital identity: the law.

[653] Robin Wilton, 'What's the Value of Your Digital Identity,' Keynote Address, OTS 2010, Maribor (June 2010) <http://www.futureidentity.eu/documents/RW-Maribor.pdf>

5. The legal regulation of digital identity: Comparative overview of the law regulating digital identity in the UK and India

> No civilization would ever have been possible without a framework of stability, to provide the wherein for the flux of change. Foremost among the stabilizing factors, more enduring than customs, manners and traditions are the legal systems that regulate our life in the world and our daily affairs with each other.
> *-Hannah Arendt*[654]

5.1. Introduction

Law is a significant regulator of digital identity.[655] This chapter, an account of the law regulating digital identity, investigates the different laws that regulate digital identity.[656] It makes a comprehensive and contemporary comparative overview of the legal regulation of digital identities in the UK and India. This is of great importance to the current and future legal scholarship in law, identity management and identity regulation, because thus far, particularly in the West, the digital identity regulatory literature has been overtly focussed on issues of digital identity from the privacy and data protection perspective. Yet, not all digital identity problems are issues of privacy and data protection.

Also, given that identity can be a global and simultaneously local phenomenon, what is the relationship between law and digital identity from the international perspective? Is it universally similar? More specifically, how does the legal regulation of digital identity occur in locally diverse jurisdictions like the UK and India? These questions form the crux of this chapter.

5.2. The law regulating digital identity

The relationship between law and digital identities is not simple; it is a complex one. This is because, just as there are many forms and natures of digital identities, there

---

[654] German-born American political philosopher, (1906-1975)
[655] L Lessig, *Code and Other Laws of Cyberspace* (Basic Books, NY 1999)
[656] How the law regulates digital identity surfaces to different degrees in the works of Beth Simone Noveck (US), The FIDIS Consortium (Europe), Roger Clarke (Australia), Paul De Hert (Brussels), Roger Brownsword (UK), Lawrence Lessig (US), P Giordano (US), Susan P Crawford (US), Josh Blackman (US), Clare Sullivan (Australia) and Sherry Turkle (US). See bibliography.

are also different laws within law,[657] with different form, substance and nature that affect digital identity.[658] This section examines the prevalent legal regulatory regime applicable to digital identity in the UK[659] and India in the following order: criminal law, law of fundamental rights and freedoms (constitutional and human rights law), law of national identity schemes, contract law, intellectual property law, tort law and data protection law.

5.2.1. Criminal law

Identity related crime[660] has by and large traditionally been subject in large part to criminal law and criminal law remains one of the significant regulators of digital identities in respect of crimes committed in connection to it. Identity related crime manifests in activities like identity fraud, phishing,[661] account hacking (unauthorised access to account), identity piggybacking (whether through account, IP address or system), man in the middle attacks,[662] pharming,[663]social engineering[664] and Sybil attacks.[665]

But how does criminal law regulate digital identity? At the international level there is no criminal framework regulating digital identity crime even though it often has trans-national implications. The only international legal instrument providing an

[657] Per Burgess, law represents, "a deep and complexly layered constellation of structures, norms, interests and authoritative practices." JP Burgess, 'Law and Cultural Identity,' ARENA Working Papers, WP 97/14

[658] Laws are largely jurisdictional creatures, with diverse form, substance, nature and enforcement.

[659] In the context of the UK, EU law (whether in the form of legislation or case law) applies to the UK by virtue of the European Communities Act 1972 and prevails unless a contrary intent is expressly expressed by the UK parliament. See *McCarthys Ltd v Smith* [1979] 3 All ER 325; *Thoburn v Sunderland City Council* [2002] 3 WLR 247. The final effect of EU law finally depends on the law of its member states. See TC Hartley, *European Union Law in a Global Context: Text, Cases and Material* (CUP, Cambridge 2004), 164

[660] Defined by Koops and Leenes as "all punishable activities that have identity as a target or a principal tool." BJ Koops and RE Leenes, 'ID theft, ID fraud and/or ID-related Crime: Definitions Matter,' (2006) 30 (9) Datenschutz und Datensicherheit, 553–556

[661] Online activity conducted to make the persons disclose personal or secret information.

[662] A situation where a fake website is substituted for a real website. See Birch (2007) **n122**, 83

[663] Pharming occurs when "a worm controls a PC to reroute a user generated banking URL request to an illegal website that looks legitimate and captures user data." Birch (2007) **n122**, 82

[664] The use of a variety of techniques to manipulate people into divulging personal or confidential information. MT Biegelman, *Identity Theft Handbook: Detection, Prevention and Security,* (John Wiley and Sons, NJ 2009)

[665] A Sybil attack occurs when "a single node presents multiple identities to other nodes in the network." Erdal Cayirci and Chunming Rong, *Security in Wireless Ad Hoc and Sensor Networks* (John Wiley and Sons, Chichester 2009), 115

international criminal law framework is the Council of Europe Convention on Cybercrime,[666] premised on the need to pursue a "common criminal policy" in the digital and technologically converged world and concerned with digital criminal offences. The Convention highlights the need for States and the private sector to cooperate in cybercrime matters[667] and makes specific mention of crimes like illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), system interference (Article 5), device misuse (Article 6), computer related forgery (Article 7) fraud (Article 8), child pornography (Article 9) and intellectual property offences (Article 10).

Regulating digital identity through criminal law is primarily a national endeavour, and there are significant differences in the approaches of different countries.[668] An overview of how criminal law regulates digital identity in the UK and India now follows.

5.2.1.1.UK

The key legislations affecting digital identity under the criminal law framework in the UK are the Computer Misuse Act 1990 (CMA 1990)[669] and the Fraud Act 2006.[670]

The CMA 1990 regulates offences relating to unauthorised computer access for identity related crime (though it does not specifically mention identity crime). It deals with offences like unauthorised access to computer material (section 1), unauthorised access with intent to commit or facilitate commission of further offences (section 2), unauthorised modification of computer material (section 3) and

[666] The Convention was signed by the UK on 23 November 2001 (unratified). It is neither signed nor ratified by India.
[667] See Covention Preamble.
[668] Bert-Jaap Koops and ors, 'A Typology of Identity-Related Crime,' (2009) 12 (1) Communication & Society, 11- 24, 13
[669] The Act followed *R v Gold* [1988] 2 All ER 186
[670] The Act extends to England, Wales and Northern Ireland and not Scotland (except s 10(1) which amends the Companies Act 1985). It repeals the deception offences in ss 15, 15A, 16, and 20(2) of the Theft Act 1968; ss 15, 15A, 16 and 19(2) of the Theft Act (Northern Ireland) 1969; ss 1 and 2 of the Theft Act 1978 and Arts 3 and 4 of the Theft (Northern Ireland) Order 1978. See Explanatory Notes to the Act.

legal procedure associated with the prosecution of these offences. Any of these acts committed in relation to digital identity would be actionable under the Act.
Before and while the CMA 1990 has been in force, other legal provisions were and have been used to deal with computer-related crime and digital identity offences like fraud.[671] The Fraud Act 2006, which came into force on 15 January 2007, provides criminal liability for identity related crime like fraud and the dishonest obtaining of services.[672] It eliminates the previously established deception offences regime,[673] and makes fraud a new distinct crime category with a wider scope.[674]

The Fraud Act 2006 provides criminal liability for fraud and dishonestly obtaining services. It covers fraud by false representation, fraud by failing to disclose information or fraud by abuse of position.[675] Per section 2, fraud by false representation occurs when a person dishonestly makes a false representation, and intends, by making the representation either to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss. All conditions being satisfied, this would cover phishing,[676] pharming and credit card fraud.[677]

When digital identity is manipulated and used to commit criminal offences, it is punishable under law and is evident in the cases of *R v Breakwell*[678] and *R v Scott*.[679] Thus, criminal law regulates digital identity in the UK.

---

[671] Eg, the Theft Acts of 1968 and 1978 and the Forgery and Counterfeiting Act 1981.
[672] This includes offences like phishing, pharming, spoofing, other identity based misrepresentations and deceptions.
[673] Specifically, ss 15, 15A, 15B and 16 of the Theft Act 1968 and ss 1 and 2 of the Theft Act 1978. The Fraud Act has been criticised for moving the focus from deception to dishonesty, its omission to specifically define of key concepts like 'fraud', 'false' or 'abuse' and the shift in the liability threshold. See M Johnson and KM Rogers, 'The Fraud Act 2006: The E-Crime Prosecutor's Champion or the Creator of a New Inchoate Offence?' (2007) 21 (3) IRLCT, 295-304; B Summers, 'The Fraud Act 2006: Has it Had Any Impact?' (2008) 75 Amicus Curiae, <http://sas-space.sas.ac.uk/dspace/bitstream/10065/1783/1/amicus75_summers.pdf.pdf>; BI Adungo, 'Will the Fraud Act 2006 'Get the Law Right?' A Study of the Effectiveness of Applying Criminal Sanctions to Penalise Fraud in the 'Commercial Sphere',' (Masters Thesis, University of Manchester 2007/08)
[675] S 1 (1)
[676] *R v Wellman* [2007] EWCA Crim 2874
[677] D Bainbridge, 'Criminal Law Tackles Computer Fraud and Misuse,' (2007) 23 (3) CLSR, 276-281, 277
[678] [2009] EWCA Crim 2298 (appeal dismissed)
[679] [2008] EWCA Crim 3201

5.2.1.2.India

Criminal law, vis a vis the Indian Penal Code 1860 (IPC)[680] and the Code of Criminal Procedure 1973 (CrPC), provides the bulwark of protection for digital identities in India and this is evident in provisions of the IPC like sections 415 (cheating), 416 (cheating by personation), 417 (punishment for cheating), 419 (punishment for cheating by personation), 468 (includes electronic forgery), 469 (forgery to harm reputation), 499 (defamation), 500 (punishment for defamation) and section 507 (criminal intimidation by an anonymous communication).[681]

In addition, the ITA 2000 (as amended by ITAA 2008) encompasses offences in relation to digital identity in Chapter XI, specifically sections 65-74,[682] and in particular section 66.

Section 66 provides that any person who either dishonestly[683] or fraudulently[684] indulges in any Section 43 acts (unauthorized access and extraction/use of data, hacking, damage or disruption, computer contamination, damages or disrupts a computer system, denies access, in a misrepresenting manner tampers or manipulates and abets such acts) shall be punishable with imprisonment of up to three years, fine extending to five lakh rupees[685] or both.

The ITAA 2008 added in sections 66A (punishment for sending offensive messages through computer resources or communication devices), 66B (punishment for dishonest possession of computer resources or devices), 66C (punishment for identity theft), 66D (punishment for computer based cheating by personation), 66E

[680] Particularly, ss 420, 463-470 on forgery.
[681] Indo-Asian News Service, 'Charges Framed Against Student For Threat Mail to Kalam,' (3 September 2009) <http://news.in.msn.com/national/article.aspx?cp-documentid=3202934>
[682] S 65 (tampering with computer source documents), S 66 (computer related offences), s 67 (punishment for publication or transmission of obscene material), s 68 (Power of Controller to give directions), S 69 (Directions for interception or monitoring), s 70 (protected systems), s 71 (penalty for misrepresentation), s 72 (penalty for breach of confidentiality), s 73 (penalty for publication of false electronic signatures), S 74 (publication of electronic signature for fraudulent purposes)
[683] Per s 24, IPC, *dishonestly* means "with the intention of causing wrongful gain to one person or wrongful loss to another person."
[684] Per s 25, IPC, *fraudulently* means "with intent to defraud but not otherwise."
[685] Approximately £7000.

(punishment for privacy violation)[686] and Section 66F (punishment for cyber terrorism).

Of the above, Section 66C is particularly noteworthy as it prescribes punishment for 'identity theft' (undefined by the Act). According to this section, any person who fraudulently or dishonestly makes use of the electronic signature, password of any other unique identification feature of any other person shall be punished with imprisonment that might extend to three years and fine extending up to one lakh rupees.[687] This section would bring within its ambit a number of unlawful acts committed in relation to digital identity.

The first successful conviction and sentencing in connection to digital identity in India under the criminal (and IT law framework) happened in the case of *State of Tamil Nadu v Suhas Katti*[688] which concerned the posting of obscene, defamatory and annoying messages about a divorcee woman in the Yahoo! message group. This was followed by *Nasscom v Ajay Sood*[689] in which the Delhi High Court declared phishing on the Internet to be an illegal act entailing an injunction and the recovery of damages.

Criminal law vis a vis the IPC has always been used by itself or in conjunction with the ITA 2000) to prosecute digital identity crime.[690] The ITA 2000, even as amended by ITAA 2008, has not been taken as strong enough to provide an effective framework for regulating digital identities due to its evolving form and unclear scope.[691]

---

[686] Privacy here has a limited ambit and specifically relates to privacy of "private parts of the body" in circumstances of reasonable expectation of privacy. See explanation to section.
[687] Approx £1500
[688] CC No. 4680/2004 5 November 2004 (AMM, Egmore)
[689] 2005 (30) PTC 437
[690] See *Katti* **n688**. Applicable sections were s 67 of ITA 2000 and ss 469 and 509 IPC
[691] G Sreekala, 'Much Hyped IT Act Stays a Dead Letter,' *Times News Network* (20 July 2006) <http://economictimes.indiatimes.com/News/Business_Law/General_Law/Much_hyped_IT_Act_stays_a_dead_letter/articleshow/1783026.cms>; P Duggal, 'Cyberlaw in India: The Information Technology Act 2000 - Some Perspectives,' (6 September 2001) <http://www.mondaq.com/article.asp?articleid=13430&print=1>; S Basu and R Jones, 'E-commerce and the Law: A Review of India's Information Technology Act 2000,' (2003) 12 (1) Contemporary South Asia, 7-24

On the whole, both in the UK and India criminal law operates well to regulate digital identity.

5.2.2. Fundamental rights and freedoms: Constitutional and human rights law

Digital identity regulation also occurs in relation to fundamental rights and freedoms principally the following key areas: right to privacy and right to freedom of speech, expression and association.[692] These fundamental rights and freedoms manifest in UK human rights law and Indian constitutional law respectively.[693]

5.2.2.1. Right to privacy

First, this section analyses the human right respect for private and family life in the context of the UK and then it analyses the constitutional right to privacy in India.

5.2.2.1.1. UK: Right to respect for private and family life

The European Convention of Human Rights (ECHR)[694] incorporates the right to respect for private and family life in Article 8, which in the European context, is the most significant digital identity impacting legal provision. Article 8 states:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

---

[692] There might be other areas of law that might apply, given the complex nature of digital identity eg, right to life, equality, cultural and educational rights.

[693] Indian constitutional law is embedded in a single, codified and fairly rigid Constitution which functions as the *Supreme Lex Loci.* Umeshwar Varma, *Law, Legislature and Judiciary* (Mittal Publications, India 1996), 21; GB Reddy and Mohd Suhaib, *Constitution of India and Professional Ethics* (IKI Publishing, New Delhi 2009), 3. Reiterated in *SR Bommai v Union of India* (1994) 3 SCC 1, *Vimal CJ Jain v Shri Pradhan* 1979 AIR 1501 and *Basheshar Nath v Commr of Income Tax* 1959 AIR 149

[694] Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. As Member of the EU Community obliged to give effect to Community law and signatory to the ECHR, the UK is obligated by the ECHR particularly post the enactment of the Human Rights Act 1998 which mandates giving effect to the ECHR in the UK. See Section 3, HRA 1998.

First and foremost, Article 8 protects and guarantees individual autonomy. This is reiterated by the statement of the European Court of Human Rights (ECtHR) in *Christine Goodwin v The United Kingdom:* "Under Article 8 of the Convention in particular… the notion of personal autonomy is an important principle underlying the interpretation of its guarantees."[695]

Article 8 includes a right to identity. This is demonstrated by the large number of cases adjudicated on various aspects of identity. For instance, *Burghartz v Switzerland* (change of family name),[696] *Bensaid v the United Kingdom* (preservation of mental stability),[697] *Pretty v the United Kingdom* (choice to end life),[698] *Odievre v France* (birth confidentiality),[699] *Smirnova v Russia* (national identity papers),[700] *KA and AD v Belgium* (right to engage in sexual relations),[701] *Jaggi v Switzerland* (attempt to establish ancestry),[702] *Mizzi v Malta* (contesting paternity)[703] and *Evans v United Kingdom* (withdrawal of consent to IVF treatment).[704]

Article 8 also protects personal data. This is evidenced by cases like *Goodwin, Klass v Germany* (covert surveillance),[705] *Leander v Sweden* (logging of personal or political background on state registers),[706] *Gaskin v the United Kingdom* (refusal of public authority to grant access to formative year records),[707] *Amann v Switzerland* (interception of telephone call and creation of card with personal information of subject in public prosecutor's office),[708] *Rotaru v Romania* (file on private life by Romanian Intelligence Service),[709] *PG and JH v the United Kingdom* (covert

[695] ECtHR, App 28957/95 (11 July 2002)
[696] **n166**
[697] (2001) 33 EHRR 10
[698] (2002) 35 EHRR 1
[699] (2004) 38 EHRR 43
[700] (2004) 39 EHRR 450
[701] ECtHR, Apps 42758/98 and 45558/99 (17 February 2005)
[702] ECtHR, App 58757/00 (13 July 2006)
[703] [2006] 1 FCR 256 354
[704] (2006) 46 EHRR 321
[705] (1978) 2 EHRR 214
[706] (1987) 9 EHRR 433
[707] (1990) 12 EHRR 36
[708] (2000) 30 EHRR 843
[709] ECtHR, App 28341/95 (4 May 2000)

surveillance)[710] and *Segerstedt-Wiberg v Sweden* (storage of personal data for national security purposes)[711] *Peck v the United Kingdom* (publication of CCTV images of person wielding knife in street)[712] and *S and Marper v the United Kingdom* (unlimited retention of personal data).[713] This further establishes the fused nature of the relationship between autonomy, identity, data protection and privacy in Europe, which might explain why the digital identity regulatory discourse in Europe has been overtly focussed on these aspects. The broad ambit of protection afforded under Article 8 makes it clear that any act in respect of an individual's digital identity that breaches private and family life would come within its scope.

The ECHR Article 8 right to respect for private and family life is incorporated into UK law by the Human Rights Act 1998 (HRA 1998), in Article 8 Part I, Schedule 1. The HRA 1998 protects this right by making it enforceable. It makes several provisions in this respect. First, it guarantees that local primary legislation must comply with the Convention right; thus any legislation going contrary to the right could be declared incompatible with the right.[714] It also makes it unlawful for public authorities to act in manners incompatible with the Convention rights. Thus, if a public authority is found to be violating the right, proceedings may be brought against it for just and appropriate relief or remedy.[715]

5.2.2.1.2. India: right to privacy

There is no explicit human or constitutional right to privacy in India. But, a constitutional right to privacy for persons[716] exists through a judicial reading of it into Article 21 (right to life or personal liberty)[717] of the Constitution of India. Most privacy cases under Article 21 relate to invasions of privacy by the State/government, as fundamental rights are primarily available against the State and

[710] [2000] ECHR 192
[711] [2007] EHRR 2 (CCHR)
[712] (2003) 36 EHRR 41
[713] [2008] ECHR 1581
[714] S 4
[715] S 8(1), HRA 1998
[716] The right to privacy was found not to exist under Article 21 for corporations. *Petronet LNG Ltd v Indian Petro Group* CS (OS) 1102/2006, 22 April 2009 (Delhi High Court) § 38
[717] Article 21 states that "No person shall be deprived of his life or personal liberty except according to procedure established by law." This is the most important fundamental right that is guaranteed against State infringement.

its agents. But fundamental rights can also be invoked against private persons as demonstrated in the cases of *Bodhisattwa Gautam v Subhra Chakraborty*[718] and *Zee Telefilms Ltd v Union of India*.[719]

The right to privacy, under Article 21, has been applied in a limited number of cases on: unlawful interference through domiciliary visits (*Kharak Singh v The State of UP*),[720] police surveillance (*Govind v State of MP*),[721] freedom of the press (*R Rajagopal v State of Tamil Nadu*)[722] telephone tapping *(People's Union for Civil Liberties v Union of India),*[723] disclosure of HIV status (*Mr 'X' v Hospital 'Z'*),[724] search and seizure provisions (*District Registrar and Collector, Hyderabad v Canara Bank)*[725] and power of the Court to direct a party to undergo a medical examination *(Sharda v Dharampal).*[726] In these cases, the right to privacy has manifested as: a right to be let alone, and a right to safeguard one's privacy and the privacy of one's family, marriage, procreation, motherhood, child-bearing and education. Though this is optimistic and might seem like Article 21 offers extremely good privacy protection to individuals, this is hardly the case.

The scope of the right to privacy under Article 21 has been strictly demarcated. The right to privacy is not an inviolable or absolute right.[727] It is always to be balanced against other rights and values as held in *Govind.*[728] In *Mr. 'X,'* [729] it was determined that the right to privacy was subject to lawful action taken for the prevention of crime, disorder, to protect health, morals or the rights and freedom of others. In the case of a conflict between two fundamental rights, it has been determined that the one which advances public morality would take precedence.[730] Courts in India in

[718] AIR 1996 SC 922
[719] AIR 2005 SC 2677
[720] (1964) 1 SCR 332. Privacy as a right to personal intimacies of the home, the family, marriage, motherhood, procreation and child-bearing.
[721] (1975) 2 SCC 148
[722] (1994) 6 SCC 632.
[723] (1997) 1 SCC 301.
[724] (1998) 8 SCC 296
[725] (2005) 1 SCC 496
[726] (2003) 4 SCC 493
[727] *KJ Doraisamy v The Asst General Manager*, WP 17761/2006 (Chennai High Court)
[728] **n721**
[729] **n724**
[730] (2003) 4 SCC 493. Supported in the *Swami Nithyanandaji Maharaj* case, CS 346/2010, (Chennai High Court).

privacy litigations have given it extremely limited berth,[731] demonstrating a strong reluctance to inflate the scope of the private sphere.[732]

The right to privacy under the Indian Constitution differs in several respects in comparison to the right to private life in the ECHR. First, the right to privacy under Article 21 is not a tool for the individual to declare or protect his autonomy[733] rather it exists to protect personal liberty[734] and dignity.[735] Second, it offers very limited theoretical protection to digital identity as there are no cases (except *PUCL*) in which it has been used to protect digital identity. In contrast, Article 8 of the ECHR has been used to protect key facets of an individual's digital identity like personal information, database identity, DNA profiles and CCTV images.

Thus, unlike the broad and robust protection offered by Article 8 in Europe and the UK, the constitutional right to privacy in India offers weak protection to individuals in respect of their digital identity.

5.2.2.2.Right to freedom of speech, expression, association and assembly

Speech, expression and association are important elements of digital identity. This section analyses what protection the law offers to these elements by virtue of fundamental rights and freedoms it provides.

In the UK, the right to freedom of expression and the right to freedom of peaceful assembly and association are two different rights under the human rights framework. In India on the other hand, the right to freedoms of speech, expression, assembly and association are embodied in a single provision in the Constitution.

---

[731] This was evident in *MP Sharma v Satish Chandra* AIR 1954 SC 300, where the Supreme Court held that "there was no justification to import the right to privacy into our Constitution by a process of strained construction."
[732] In *Petronet,* only health, personal relationships and finances were brought within the scope of the private sphere envisaged under Article 21.
[733] The Indian Constitution does not deny the place of individual autonomy; rather recognises it only in a limited role. *Govind* **n721** § 23
[734] See comments of VR Krishna Iyer, LJ (concurring) in *Maneka Gandhi v Union of India* (1978) 1 SCC 248. "The spirit of man is at the root of Article 21. Absent liberty, other freedoms are frozen."
[735] (1975) 2 SCC 148

5.2.2.2.1. UK

The right to freedom of expression and the right to freedom of peaceful assembly and association are now analysed.

5.2.2.2.1.1.Right to freedom of expression

The right to freedoms of expression, as found in Article 10 of the ECHR,[736] is enshrined in Article 10, Part I, Schedule 1 of HRA 1998 which gives effect to it. According to this right, a person is entitled to hold opinions, receive and impart information and ideas without interference by public authorities, regardless of frontiers subject to such formalities, conditions, restrictions or penalties as are prescribed by law and necessary in a democratic society. For instance, an individual has the right to share his opinions on Twitter,[737] receive tweets and follow other Twitters, subject to reasonable restrictions as imposed by the site or law.

The importance of the freedom of expression in the UK was summed up in *Regina v Secretary of State for Culture, Media and Sport*:[738]

> Freedom of thought and expression is an essential condition of an intellectually healthy society… These are the values which article 10 exists to protect, and their importance gives it a central role in the Convention regime, protecting free speech in general and free political speech in particular.

States are obliged to ensure non-interference with the right to freedom of expression as well as take positive steps to ensure its availability and enjoyment.[739]

---

[736] Article 10 ECHR states:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[737] <http://twitter.com/>

[738] [2008] 1 AC 1312, para 27

[739] *Özgür Gündem v Turkey*, ECtHR, App 23144/93 (16 March 2000), paras 42-46; *Fuentes Bobo v Spain*, ECtHR, App 39293/98 (29 February 2000), para 38

5.2.2.2.1.2.Right to freedom of peaceful assembly and association

The right to freedom of peaceful assembly and association, as mandated by the ECHR, is enshrined in Article 11, Part I, Schedule 1 of the HRA 1998. This provision enables an individual to further socially mediate digital identity. An individual may join a group on Facebook or participate in a digital forum. Any restrictions on this right can only be such as are prescribed by law and necessary in a democratic society.

These provisions are only some of the main provisions that apply regulate digital identity under the human rights regime in the UK which illustrate that there is a well established mandate for the regulation of digital identity under this regime.

5.2.2.2.2. India: Right to freedom of speech, expression, assembly and association

Much like the fundamental rights and freedoms enjoyed under the ECHR, the fundamental rights of speech, expression, assembly and association are available to Indian citizens in respect of their digital identity.

Article 19 of the Constitution inter alia guarantees to Indian citizens a right to freedom of speech and expression, to assemble peaceably and without arms and to form associations or unions.[740] Indian digital identity subjects, per this Article, are able to freely express, develop and propagate their digital identities in any lawful form or manner. They are free to associate with other digital identities. This right can be enjoyed "untrammelled by unreasonable Governmental restraint,"[741] subject to reasonable restrictions.[742] If any of the freedoms embodied in Article 19 are infringed, deprived or curtailed then a holder of the right is entitled to relief in law.[743]

---

[740] Per Art 19(2) these are: sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order, decency or morality, contempt of court, defamation or incitement to an offence.

[741] *Lakshmi Ganesh Films v Government of AP* 2006 (4) ALD 374

[742] Art 19(2)

[743] See *State of Gujarat v Mirzapur Kassab* [2005] RD-SC 602*, Om Kumar v Union of India* (2001) 2 SCC 386, *Romesh Thapar v Madras* AIR 1950 SC 124*, Express Newspapers v Union of India* (1985) 1 SCC 641*, Sakal Newspapers v Union of India* AIR 1973 SC 112 and *Bennet Coleman and Co. Ltd. v Union of India* 1973 AIR 106

From the above account, it is evident that both UK and India provide fundamental rights and freedoms that apply in respect of digital identity. While the right to privacy manifests difference in its nature and scope, the right to freedoms of speech, expression and association are highly similar.

5.2.3. Law of national identity schemes

One of the most prominent manners in which the law impacts digital identity is through the establishment and regulation of national identity schemes. National identity schemes are schemes of identity establishment, authentication and verification established by a national government, intended to serve as instruments of citizenship management and facilitate effective governance. Both the UK[744] and India[745] have evidenced intent of regulating identity through the establishment of such schemes.

5.2.3.1.UK

The Identity Cards Act 2006[746] was enacted as an enabling Act to establish a National ID cards scheme in the UK.[747] It aimed to

> make provision for a national scheme of registration of individuals and for the issue of cards capable of being used for identifying registered individuals; to make it an offence for a person to be in possession or control of an identity document to which he is not entitled, or of apparatus, articles or materials for making false identity documents...[748]

The repealed Act[749] made provisions for a National Identity Register (NIR) to function as a "secure and reliable record of registrable facts about individuals in the UK" that would serve prescribed statutory purposes (provision of a convenient method for individuals to prove registrable facts about themselves to others and

[744] ie, the National Identity Cards Scheme
[745] ie, the Indian UID Scheme
[746] Obtained Royal Assent on 30 March 2006.
[747] Not entirely a new development, as ID cards schemes were implemented from 1915-1919 and 1939-1952 (enabled by National Registration Act 1939 and Emergency Registration Act 1939)
[748] Preamble
[749] Repealed by the Identity Documents Act 2010.

provision of a secure and reliable method for registrable facts to be ascertained or verified where necessary in the public interest).[750]

Sections 25 (possession of false identity document), 26 (identity documents) and 38 of the Identity Cards Act 2006 still apply.[751] These are incorporated in the Identity Documents Act 2010. Section 4 (1) criminalises the possession of a false identity document. Section 7 (1) lists what are identity documents: immigration documents, UK or international passports, identity documents used instead of passports, UK or international driving licences. According to Section 4(1) it is an offence for a person, with "improper intention"[752] to possess or control a false identity document known or believed to be false, an improperly obtained identity document, or an identity document relating to another person. Also criminalised are the possession of apparatus for making false identity documents (section 5) and possession of false identity documents without reasonable excuse (section 7).

5.2.3.2.India

The Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules 2003[753] provide for the establishment and maintenance of a national identity register of citizens[754] containing the following information: name, parents names, sex, date and place of birth, residential address (present and permanent), marital status, name of the spouse, visible identification mark, date of registration of citizen, serial number of registration and National Identity Number (now called the *Aadhaar* Number).[755] The Rules also provide for the issue of National Identity Cards by the Registrar General of Citizen Registration to every citizen registered on the National Register of Indian Citizens.[756]

---

[750] S 1
[751] Identity Documents Act 2010, s 1(2)
[752] S 4(2)
[753] Notified in Government of India Gazette, GSR No. 937(E) (10 December 2003)
[754] Rule 3(1)
[755] Rule 3 (3)
[756] Rule 13

Rule 14 imposes obligations in relation to ID Cards. The identity card remains the property of the Central Government.[757] Rule 14 (2) prescribes that no person shall wilfully destroy, alter, transfer or use in any form the National Identity Card, except for the lawful purposes. Rule 14(3) prescribes that the identity card of an individual must be surrendered in case the following occurs: death, cessation of citizenship, revocation of citizenship or discovery of incorrect particulars.

The Rules also prescribe penal consequences (in the form of a fine extending up to one thousand rupees)[758] for a violations of the following Rules: Rule 5 (preparation of database), 7 (initialisation of the Register and registration), 8 (determination of citizenship status), 10 (deletion of name and particulars from the Register), 11 (maintenance and updating of the Register) and 14 (duty to keep ID cards safe).

Under these Rules, India piloted the Multi-purpose National Identity Card (MNIC) Scheme, which evolved into the Unique Identity (UID) Scheme. The UID Scheme (initially non-compulsory), rolled out in September 2010,[759] is targeted at Indian residents and seeks to provide them a random unique number of identification. The Scheme aims at facilitating the delivery of public sector goods, services and the maintenance of national safety and security through providing residents of India with an effective means of establishing, authenticating and verifying identity.

The Unique Identification Authority of India (UIDAI),[760] to be set up as a statutory authority called the National Identification Authority of India (NIDAI), will oversee the setting up of the Scheme, the issue of the Aadhaar numbers and the regulation of the Scheme. On 24 September 2010, the Cabinet approved a proposal for the National Identification Authority of India Bill 2010[761] to be introduced in

[757] Recall here how an individual's identity may only be 'possessed' or 'assigned' **Ch 2 (2.5.6)** and Also **Ch 2 (2.5.7)**
[758] Rule 17
[759] UIDAI, 'National Launch of the Aadhaar Project,' <http://uidai.gov.in/images/FrontPageUpdates/pressnotefinal.doc>
[760] <http://uidai.gov.in/>
[761] Draft Bill: <http://uidai.gov.in/documents/NIA%20Draft%20Bill.pdf>

Parliament.[762] The draft Bill does not define an individual's identity, rather defines "identity information" of an individual as "biometric information, demographic information and Aadhaar Number."[763]

According to the Bill,[764] every resident shall be entitled to obtain an *Aadhaar* number (which will function as proof of identity subject to authentication) on providing his demographic information and biometric information, which shall be issued by the NIDAI after verifying the information, in prescribed manner. The identity data would be stored on the Central Identities Data Repository (CIDR).

The Bill makes provisions for identity related offences like identity impersonation at enrolment,[765] impersonation of *Aadhaar* number holder,[766] unauthorised collection of identity information under the Scheme,[767] unauthorised disclosure of identity information,[768] unauthorised access to the CIDR,[769] tampering with data in the CIDR[770] and the manipulation of biometric information.[771] The Bill also seeks to impose a general penalty for offences not provided for under the Act and committed in relation to it.[772]

Thus, we see how law regulates identity under specific national identity schemes.

---

[762] Press Information Bureau, 'Approval for Introducing the National Identification Authority of India Bill 2010 in Parliament,' (24 September 2010) <http://pib.nic.in/newsite/pmreleases.aspx?mincode=61>.The Bill was available online for public consultation in July 2010.
[763] The National Identification Authority of India Bill 2010, s 2(k)
[764] The Bill aims "to provide for the establishment of the National Identification Authority of India for the purpose of issuing identification numbers to individuals residing in India and to certain other classes of individuals and manner of authentication of such individuals to facilitate access to benefits and services to such individuals to which they are entitled and for matters connected therewith or incidental thereto." *Preamble.*
[765] S 34
[766] S 35
[767] S 36
[768] S 37
[769] S 38
[770] S 39
[771] S 40
[772] S 41

5.2.4. Contract law

Contract law represents another potent means of regulating digital identity. Contract law regulates digital identity through laws regulating electronic signatures, ID certificates, terms of service and agency.

5.2.4.1.Electronic signatures

One of the most visible and developed form of legal regulation of digital identities is manifested in the law relating to electronic signatures. Over fifty countries have enacted and others are in the process of enacting laws relating to electronic signatures.[773]

The first international initiative in this respect was the UNCITRAL Model Law on Electronic Commerce[774] which provides the terms under which legal requirements were met in relation to data messages. Article 7 (1) provides that the legal requirement for a signature is met in relation to a data message if (a) a method is used to identify that person and to indicate that person's approval of the information contained in the message, and (b) if the method is as appropriately reliable in terms of the purpose of the generation and communication of the message and its underlying agreement. This was followed by the UNCITRAL Model Law on Electronic Signatures 2001[775] which aims to give additional legal certainty to the use of electronic signatures and establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures.

In the EU, the Electronic Signatures Directive[776] paved the way for EU Member States to harmonise their national laws in relation to electronic signatures. Here,

[773] Lorna Brazell, *Electronic Signatures Law and Regulation* (Sweet and Maxwell, London 2004)
[774] Adopted 12 June 1996.
[775] This law follows a technology neutral approach.
[776] Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community Framework for Electronic Signatures, OJ L 013, 19/01/2000 P 0012 – 0020

along with a definition of electronic signatures,[777] there is also a definition of 'advanced electronic signatures.'[778]

5.2.4.1.1. UK

In the UK, the relevant legislation governing electronic signatures are the Electronic Communications Act 2000 (ECA) and the Electronic Signatures Regulations 2002 (ESR).[779] Section 7 of the ECA speaks of electronic signatures and certificates. Section 7 (1) deals with the admissibility of electronic signatures in legal proceedings and section 7(2) broadly conceptualises electronic signatures as anything in electronic form that

> (a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and
> (b) purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both.

The ESR set out definitions of electronic signatures in conformity with the definitions set out in Section 2 of the EU Electronic Signatures Directive. It has been argued that the UK adopts a 'minimalist approach' to regulating electronic signatures.[780] The minimalist approach envisages a technologically neutral approach with no particular form of technology taking precedence over the other (with market determining which technology flourishes and with the intent of enabling technological innovation and catering for global differences).

5.2.4.1.2. India

In India, the ITA 2000[781] limitedly provided for digital signatures and not electronic signatures. A digital signature was defined as "authentication of any electronic

---

[777] Defined in Art 2(1) as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication." Art 2 (1).
[778] Defined in Art 2(2) as an electronic signature meeting the following requirements: it is uniquely linked to the signatory, is capable of identifying the signatory, is created using means that the signatory can maintain under his sole control and is linked to the data to which it relates in a manner such that any subsequent change in the data is detectable.
[779] Enacted to implement the EU Electronic Signatures Directive.
[780] M Wang, 'Electronic Signatures,' (2007) 23 (1) CLSR, 32-41, 33
[781] Ss 2, 4, 5, 14, 15 and Chapter IV.

record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3."[782] Section 3 provides the means of authenticating electronic records: by affixation of digital signature, by the use of an asymmetric crypto system and by the use of the subscriber's public key. Section 5 provides for the legal recognition of digital signatures.[783]

The ITAA 2008 introduced the wider concept of 'electronic signature' (based on the UNCITRAL Model Law on Electronic Signatures 2001) to substitute and include 'digital signatures.' [784] Here, an electronic signature is defined as "authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature."[785]

An electronic record may be authenticated by an electronic signature or electronic authentication technique that is reliable and specified in the Second Schedule.[786] An electronic signature or electronic authentication technique is considered authentic if: the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person; the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person; any alteration to the electronic signature made after affixing such signature is detectable; any alteration to the information made after its authentication by electronic signature is detectable; and it fulfils such other conditions which may be prescribed.[787]

---

[782] S 2 (1) (p)
[783] S 5 of the Act provides that, "Where any law provides that information or any other matter shall be authenticated by affixing the signature, or any document should be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by the means of digital signature affixed in such manner as may be prescribed by the Central Government."
[784] D Chansoria and R Asoka, 'Digital Signature: Strategic Shift from 'Form' to 'Function'' (2004) 17 CILQ, 269-280, 276
[785] S 2 (ta) inserted into the principal Act.
[786] Not specified as at 1.12.10
[787] S 3(A). The provision resonates much of the substance of the EU Electronic Signatures Directive, Art 2(2)

Thus, both in both the UK and India, electronic signatures have legal effect and are legally admissible, and to a large extent both countries follow a technology neutral approach.

5.2.4.2.ID certificates

Law regulates the use of digital ID certificates issued by Certification Authorities. Digital ID certificates are largely governed by the contractual relationship between the holder and certificate issuer and therefore covered here.[788]

5.2.4.2.1. UK

At the EU level, the EU Electronic Signatures Directive sets out the requirements for digital certificates. Per the Directive, a certificate refers to "an electronic attestation which links signature-verification data to a person and confirms the identity of that person."[789] It also defines qualified certificates, which are certificates that fulfill the conditions set out in Annex I of the Directive and provided by a certification-service-provider fulfilling the requirements laid down in Annex II.[790]

The Directive provides that certificates may be used as confirmation of electronic signatory's identity.[791] It qualifies the use of pseudonyms in certificates - the use of pseudonyms in certificates shall not prevent any Member State from calling for the identification of persons in conformity with either Community or national law.[792] Article 3 exhorts EU Member States to establish appropriate certification systems both in terms of supervision of certification-service-providers established on its territory and for the issue of qualified certificates to the public. There are also provisions on liability in Article 6.

---

[788] Digital ID certificates may also be subject to consumer protection law and in cases where no contract is evident, to tort law especially as regards liability. In respect of tort law see A Michael Froomkin, 'The Essential Role of Trusted Third Parties in Electronic Commerce,' (1996) 75 Ore L Rev 49

[789] Art 2(9)

[790] See Art 2 (10) & (11)

[791] Recital 20

[792] Recital 25

It is relevant here to note the divergence in the UK regime on Article 6. The ESR 2002 provide for the liability of certification-service-providers. Regulation 4 states that if a person reasonably relies on a guaranteed qualified certificate (either for its accuracy, inclusion of Schedule 1 details, signature-creation data, or the ability of the signature-creation data and the signature-verification data to be used in a complementary manner in cases where the certification-service-provider generates them both) and suffers a loss as a result, then the certification-service-provider would be liable in damages for any loss if a duty of care is found to exist and the certification-service-provider was negligent. This liability arises even if there is no proof of the certification-service-provider's negligence unless the certification-service-provider can prove no negligence.

The Electronic Signatures Directive also provides that in the case of qualified certificates issued by certification-service-provider established in a third country, Member States are to ensure that these are given equal status to certificates issued by a certification-service-provider established within the Community, on fulfilment of one of the prescribed conditions.[793]

There are also data protection provisions in relation to digital certificates in the Directive. For example, Art 8(2) states that certification-service-provider issuing certificates may collect personal data only directly from the data subject or after the explicit consent of the data subject, and only data necessary for the purposes of issuing and maintaining the certificate. Such data cannot be collected or processed for any other purposes without the explicit consent of the data subject. More importantly, the Directive states that Member States may not prevent certification service providers from using pseudonyms instead of signatory's names in certificates.[794]

---

[793]See Art 7 (1). The conditions are (a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or (b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or (c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

[794] Art 8 (3)

5.2.4.2.2. India

There is a strong regulatory mechanism in place for electronic (including digital) certificates in India. This is evident in Sections 17-39 of the ITA 2000 (as amended by ITAA 2008), the Information Technology (Certifying Authorities) Rules 2000 and the Information Technology (Certifying Authorities) Regulations 2001.

The Controller supervises the Certifying Authorities, lays down their duties, certifies their public keys, lays down standards to be followed, specifies the qualifications and experience of employees of Certifying Authorities**,** specifies the contents of certificates and keys, monitors accounts, regulates the Certifying Authorities' dealings with subscribers, and resolves disputes between them.[795] The Act also provides for the recognition of international Certifying Authorities by the Controller subject to law by prior approval of the Central Government and notification in the Official Gazette.[796]

Any person can apply for a licence to issue electronic signature certificates i.e. to become a Certifying Authority on fulfilment of prescribed conditions. Certifying Authorities (and their employees or agents) must ensure compliance with the Act and must under Section 30 of the Act use appropriate, safe and secure technology and procedures, provide reasonable reliability, maintain sufficient secrecy and privacy, and function as repositories of the certificates and make suitable notifications of practices and certificate statuses. The Act also prescribes duties for subscribers of certificates.[797] Unlike the UK, there are no data protection provisions. Overall, the law regulating ID certificates in UK and India is reasonably similar with some differences. In both cases ID certificates function as confirmation of signatory's identity. However, the variances are in the data protection and pseudonymity provisions in the UK.

[795] S 18, ITA 2000
[796] S 19
[797] S 40A, ITAA 2008

5.2.4.3.Terms of Service and End User Licence Agreements

The regulation of digital identity is also evident in Terms of Service (TOS) or End User License Agreements (EULAs). Most TOS and EULAs are standard form contracts. TOS or Terms of Use (TOU) refer to the agreement governing use of a service and a EULA sets out the contractual nature between the author/manufacturer of software and the user.

Identity service providers have TOS that govern their relationship with their users. For instance, ClaimId has Terms of Service that regulates how users conduct themselves, use their digital identities, limit ClaimId's liabilities, provide for conflict resolution and proprietary rights.[798] Other identity providers have similar policies.[799]

A conflict arising out of any digital identity matters governed by a legal contract will be resolved by the terms of that contract.[800] For instance, if an identity provider unilaterally deprives a digital identity subject of the use of their digital identity without notice or other due cause such that it is in breach of the contract between the two, the dispute will be settled in accordance with the contract that governs the relationship between them. The aggrieved party may sue the party in breach for compensation for the breach or for specific performance.

5.2.4.3.1. UK

The Electronic Commerce (EC Directive) Regulations 2002,[801] applicable to information society services, set out the requirements for the electronic contracts in

---

[798] <http://claimid.com/terms>

[799] See Microsoft Service Agreement, <http://explore.live.com/microsoft-service-agreement?ref=none>; AOL Terms of Use, <http://about.aol.com/aolnetwork/aolcom_terms>; Yahoo! 'Terms of Service' <http://info.yahoo.com/legal/uk/yahoo/utos-173.html>; Google, 'Terms of Service,' http://www.google.co.uk/accounts/TOS>, University of Cambridge, 'The Raven/Shibboleth Service: Terms and Conditions,' <http://www.cam.ac.uk/cs/raven/shib-terms.html>

[800] Note that the efficacy of contract law in governing Internet based contracts has come under scrutiny on many occasions. See RA Hillman and JJ Rachlinski, 'Standard-Form Contracting in the Electronic Age,' (2002) 77 NYUL L Rev, 429; Mark Lemley, 'Terms of Use,' (2006) 91 Minn L Rev 459

[801] The Regulations implement Arts. 3, 5, 6, 7(1), 10 to 14, 18(2) and 20 of the Directive on Electronic Commerce. Questions relating to information society services are covered by the Data Protection Directive, the Telecommunications Data Protection Directive and the Directive on Privacy and Electronic Communications and thus excluded from the scope of the Regulations.

the UK. As per the Regulations, for an electronic contract to be valid, it must have been provided to the digital identity subject by a service provider prior to use of services and must in clear, comprehensible and unambiguous manner,[802] provide the following information:

> (a) The different technical steps to follow to conclude the contract;
> (b) Whether or not the concluded contract will be filed by the service provider and whether it will be accessible;
> (c) The technical means for identifying and correcting input errors prior to the placing of the order; and
> (d) The languages offered for the conclusion of the contract.

The Regulations also provide that a service provider must indicate the relevant codes of conduct he subscribes to and give information on how those codes can be consulted electronically.[803] Where the service provider makes terms and conditions applicable to the contract to the identity subject, the service provider must make them available to the identity subject in a manner that allows him to store and reproduce them.[804]

5.2.4.3.2. India

The Indian Contract Act 1872 (subject to the provisions of the ITA 2000, specifically sections 10, 12 and 13) regulates TOS and EULAs.[805]

TOS and EULAs to be enforceable must be valid contracts i.e. they must fulfil the following certain conditions. There must be an offer (not just an invitation to offer), acceptance of offer, lawful consideration, intention to create legal relations, competency to contract, free and genuine consent, lawful object for the contract, and the certainty, possibility of performance and not expressly declared to be void.[806] If a TOS or EULA fulfils these conditions, it would be enforceable in respect of digital identity.

---

[802] S 9 (1)
[803] S 9 (2)
[804] S 9 (3)
[805] Provisions of general legislation have to be interpreted harmoniously with specific legislation.
[806] S 10, ICA 1872

Section 10A of the ITA 2000 (as amended by ITAA 2008) makes electronic contracts legally enforceable. Section 12 deals with the acknowledgment of receipt of electronic record. Where not stipulated, an electronic record is deemed to be received if either its receipt is acknowledged by communication from the addressee or the by conduct of the addressee that indicates so.[807] Section 12 also provides that where stipulated that electronic record would be binding only on receipt of an acknowledgment of electronic record, then unless acknowledgment is received, the electronic record shall be deemed to have been never sent by the originator.[808] Section 13 deals with the time, place of dispatch and receipt of electronic record.[809]

Thus, both in the UK and India, any contracts made in respect of digital identity services would be regulated by law, either through specific provisions or the general law of contract.

5.2.4.4.Agency

Agency is another vital area of contract law that impacts digital identity. The law of agency is expressed in the Latin maxim of *qui facit per alium, facit per se*, i.e. one who acts through another, acts in his or her own interest. In the doctrine of agency there are two parties – the principal and the agent. The principal is the person on whose behalf the agent acts. The agent refers to the person employed or engaged by the principal to act on his or her behalf.

Under the law of contract, if a person X makes a contract with person Y on behalf on person Z, then the law of contract presumes that a contract exists between Y and Z. Here X was an agent of Z and acted on his behalf. The law makes a presumption that X and Z are acting as one person, provided that X had due authority to make that contract on behalf of Z.[810]

---

[807] S 12 (1) (a) & (b)
[808] S 12 (2). Vide ITAA 2008
[809] It states that the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator (s 13 (1); An electronic record is deemed to be dispatched at the place where the originator has a place of business, and to be received at the place where the addressee has its place of business (s 13 (3).
[810] For detailed exposition of UK contract law, see PS Atiyah and S Smith*, Introduction to the Law of Contract* (OUP, Oxford 2006) and HL MacQueen and J Thomson, *Contract Law in Scotland* (Bloomsbury Publishing, Haywards Heath 2007); for the Indian perspective see TR Desai, *The Indian Contract Act and The Sale of Goods Act* (Lexis Nexis Butterworths Wadhwa, Nagpur 2009).

This can be extended to the digital identity context. A digital identity subject might contractually consent to a digital identity management provider making or taking certain decisions on its behalf. In such cases, the digital identity subject and the digital identity provider could be presumed to be one and the same person, and the digital identity subject would incur liability for any actions that its agent (the digital identity provider) might have taken. Thus, an agent's acts would bind the principal.

Some jurisdictions expressly provide for the recognition of electronic agency. For instance, The Electronic Transactions Act 1999 of Bermuda;[811] the Uniform Electronic Transactions Act 1999 (UETA)[812] and the Electronic Signatures in Global and National Commerce Act (ESIGN)[813] in the US. This section now examines the position of the law in the UK and India.

5.2.4.4.1. UK

The principles of agency were enumerated in a number of English cases. According to *Salomons v Pender,*[814] an agent must not betray the confidence a principal reposes in him in respect of his skill, diligence and zeal and to his own advantage. In *Boston Deep Sea Fishing v Ansell,*[815] it was held that an agent who misconducts himself in respect of his agency gives his principal (whether a company or and individual) the power and authority to relieve him of his agency.[816] In *Andrews v Ramsay,*[817] it was upheld that an agent has a duty to act in good faith towards his principal.[818] An agent's fiduciary duties were examined comprehensively in *Imageview Management Ltd v Jack.*[819]

[811] Part I, 2; S 16 (1)
[812] S 2 (6); S 14
[813] Enacted on 30 June 2000, ESIGN provides in S 101(h) that "A contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound."
[814] (1865)1 H&C 639
[815] (1888) 39 Ch D 339
[816] Per Cotton LJ, 357
[817] [1903] 2 KB 635
[818] *Rhodes v Macalister* (1923) 29 Com Cas 19
[819] [2009] EWCA Civ 63

Though there is no express legislation governing electronic agency, it has been suggested, per *Thornton v Shoe Lane Parking*,[820] that a contract formed without human intervention could be a valid contract and enforceable as such.[821]

5.2.4.4.2. India

The Indian Contract Act 1872 deals with agency in Chapter X.[822] Any person of the age of majority and sound mind can be an agent, [823] and any person of the age of majority, of sound mind may employ an agent.[824] There is no need for any consideration to establish the relationship of agency.[825] An agent's authority may be expressed or implied.[826] It has authority to act lawfully on behalf of the principal.[827] In conducting the principal's business, the agent must act according to the principal's directions or in the absence of any such directions, according to the common customs that prevail in the business or at the place where the business is conducted.[828] If the agent acts otherwise, and the principal incurs a loss, then the agent must make good such loss to the principal. If a profit accrues, it must be accounted for.
There are several other provisions that govern the principal-agent relationship. An agent must act with skill and reasonable diligence or make compensation to his principal in respect of the direct consequences of his own neglect, want of skill or misconduct, but not in respect of loss or damage which is indirectly or remotely caused by such neglect, want of skill or misconduct.[829] The agent also has a duty to communicate with the principal,[830] and act on the principal's behalf in an emergency.[831]Agency may be terminated either by the principal revoking his authority; or by the agent renouncing the business of the agency; or by the business

---

[820] [1971] 2 QB 163
[821] Graham JH Smith, *Internet Law and Regulation* (Sweet and Maxwell, London 2007), 818
[822] S 182 defines the terms agent and principal. An agent is "a person employed to do any act for another or to represent another in dealings with third persons. The principal is "the person for whom such act is done, or who is so represented." S 183 provides that any person of the age of majority, of sound mind may employ an agent.
[823] S 184, ICA 1872
[824] S 183
[825] S 185
[826] S 186
[827] S 188
[828] S 211
[829] S 212
[830] S 214
[831] S 189

of the agency being completed; or by either the principal or agent dying or becoming of unsound mind; or by the principal being adjudicated an insolvent under the provisions of any Act for the time being in force for the relief of insolvent debtors.[832] The ICA 1872 also provides for conditions under which a person may expressly or implicitly ratify acts done on his behalf.[833]

There is no express provision or case law on electronic agency in India.

Thus, is evident how closely similar the contractual regimes regulating digital identity in the UK and India are.

5.2.5. Intellectual property law

Digital identity is also affected by intellectual property law[834] in its various forms: law of trademarks, domain names, passing off, copyright and the law of confidence.

5.2.5.1.Trademarks

A trademark is defined in Article 15(1) of the TRIPS Agreement[835] as "any sign, or any combination of signs, capable of distinguishing the goods or services of one undertaking from those of other undertakings." A trademark can take any form: personal names, letters, numerals, figurative elements and combinations of colours as well as any combination of such signs. A digital identity of such nature would merit protection under trademark law.

Digital personality forms an important aspect of digital identities, for instance, one's digital names, images or likeness. These identities develop reputation, goodwill and

---

[832] S 201
[833] Ss 196-198
[834] Intellectual Property Law in England and Scotland is essentially similar due to the shared nature of legislation at EU and UK levels e.g. the Patents Act 1977, the Copyright, Designs and Patents Act 1988 and the Trade Marks Act 1994. See DL Carey Miller and MM Combe, 'The Boundaries of Property Rights in Scots Law,' Report to the XVIIth International Congress of Comparative Law, (2006)10 (3) EJCL <www.ejcl.org/103/art103-4.doc>
[835] Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994.

economic value becomes attached to them. When the "use of the true identity of an individual" is made in the "marketing or advertising of goods or services,"[836] it is termed as personality merchandising, and the law of trademarks is used to protect it.

Trademark law ensures that trademarks (registered or unregistered) are afforded suitable protection to protect the goodwill and reputation attached to them. Trademarks grant an unlimited monopoly in their use, as opposed to other forms of intellectual property with fixed term (though trademark registration lasts only for a specific period of time – ten years in the UK and India).

5.2.5.1.1. UK

In the UK, trademark[837] law has been invoked in context of the Internet in cases like the *1-800-Flowers Inc v Phonenames Ltd* (distinctiveness and illegality in use of name),[838] *Euromarket Designs Incorporated v Peters* (infringement through use of name in advertisement/ application of own name defence)[839] and *Speechworks Limited v Speechworks International Incorporated* (interim interdict for website, global effects).[840]

Personal names used in the course of trade have merited trademark protection.[841] In *Nichols Plc v Registrar of Trademarks,*[842] it was held that a surname was capable of constituting a trademark. Applying this principle, it can be said that a digital name, if used in the course of trade and satisfying conditions stipulated, would be protected under the law of trademarks.

---

[836] JN Adams, *Character Merchandising* (LexisNexis, UK 1996), xiv
[837] The UK definition of trade marks is similar to the Community definition.
[838] [2001] EWCA Civ 721
[839] [2000] EWHC Ch 179
[840] [2000] ScotCS 200
[841] eg, Marilyn Monroe (TM 1308828), Gucci, Dior, Versace, Naomi Campbell. See also *International Madrid (UK) Case* M706887.
[842] [2005] All ER (EC) 1

Images have also been afforded protection,[843] as have signatures[844] especially in the case of famous individuals, if prescribed conditions exist. Digital images would also be subject to similar protection.

5.2.5.1.2. India

Trademark law has similarly been brought into play in the digital context in India. Courts have ruled that the Internet based goods and services are entitled to trademark protection.[845] In the case of *Mattel Inc and Ors v Jayant Agarwalla,*[846] relating to the infringement of the Scrabble trademark by a company launching the "Scrabulous" application on Facebook and promoted on similarly named websites and metatags. It was ruled that Scrabble was not a generic term and that the term Scrabulous was too phonetically and semantically similar, not original and attracted people looking for Scrabble, thereby infringing Scrabble's trademark.

The 'Microsoft' trademark has also been actioned for infringement. One example is *Microsoft Corporation v Deepak Raval,*[847] which related to the infringement of the Microsoft trademark through counterfeiting and pirating of Microsoft hardware and software, where a decree for damages was passed.[848] Similarly, in *Infosys Technologies Limited v Pravarthan Infosys Pvt Ltd* [849] the infringing use of the "Infosys" brand on a website was stopped. In *Yahoo, Inc v Sanjay V Shah,*[850] the malafide use of "Yahoo!" was acknowledged and damages were awarded.

Both in UK and India, a name is not per se registrable as a trademark. The Indian position is that personal names or surnames are not prima facie registrable unless

---

[843] *Rowland v Mitchell* (1897) 14 RPC 37; Also as done by Eric Cantona (UK TM 2120277), Damon Hill (UK TM 2036489)
[844] For instance, Marilyn Monroe (UK TM 2142860), James Dean (UK TM No 1289838); *Elvis Presley Enterprises Inc v Sid Shaw Elvisly Yours* [1999] RPC 567
[845] *Tata Sons Ltd v Manu Kosari* 2001 PTC 432 (Del)
[846] CS (OS) 344/2008, 17 Sept 2008 (Delhi High Court)
[847] 2006 (33) PTC 122 (Del)
[848] In similar vein see *Microsoft Corporation v A Jain* CS (OS) 967/2007(Del); *Microsoft Corporation v Kiran* 2007 (35) PTC 748 (Del); *Microsoft Corporation v K Mayuri* 2007 (35) PTC 415 (Del); *Microsoft Corporation v Yogesh Popat* 2005 (30) PTC 245 (Del); *Microsoft Corporation v Kamal Vahi* CS (OS) 817/2004 (Del); *Microsoft Corporation v Akram Khan* CS (OS) 117/2003(Del); *Microsoft Corporation v Rajender Pawar* CS (OS) 530/2003 (Del); *Microsoft Corporation v Rahul Pachpore* CS (OS) 2428/1999 (Del)
[849] Delhi High Court, 20 Feb 2006
[850] 128 (2006) DLT 488

distinctiveness can be proved (courts will consider the extent and peculiarity of the distinctiveness, the future probability of distinctiveness being maintained, nature of use, and extent to which granting the monopoly would restrict the freedom of others with the same names to exercise their rights to such).[851]

Thus, in respect of trademark law, in both UK and India, it has been similarly employed to protect goodwill and reputation of commercial digital identity.

5.2.5.2.Domain names

The domain name system (DNS) at the international level is administered by ICANN.[852] ICANN has a Uniform Domain-Name Dispute Resolution Policy (UDRP), assumed by registrars in all generic top level domains (e.g. .asia, .net, .com, .biz, etc) and used to deal with disputes arising out of domain name misuse as a preferred alternative to court based litigation. Common domain name disputes[853] are cyber squatting,[854] concurrent name disputes[855] and gripe sites.[856]

5.2.5.2.1. UK

In the UK, domain name cases have been dealt with under trademark law i.e. the Trademarks Act 1994, sections 10(2)[857] and 10(3)[858] and the law of passing off; evident in the *British Telecommunications*[859] and *Global Projects*[860] cases. In both

[851] *Per Burford's Application* (1919) 36 RPC 139, 150
[852] See ICANN <http://www.icann.org/>. See PB Gola, *ICANN: The Introduction of New Top Level Domains (.Info, .Biz, .Name, .Museum, .Aero, .Coop, .Pro) Under the Aspects of Trademark Law And Unfair Competition* (University of California, Los Angeles 2002)
[853] For comprehensive coverage of domain name disputes, see RA Badgley, *Domain Name Disputes* (Aspen Law & Business Publishers, NY 2002)
[854] Cybersquatting occurs when a domain name is appropriated in bad faith to gain economic advantage.
[855] Concurrent name disputes occur when two parties claim rights to the same domain name.
[856] Gripe sites are offending domain names.
[857] *Phones4U Ltd v Phone4u.co.uk Ltd* [2006] EWHC Civ 244; *Ellerman Investments Limited v Elizabeth C-Vanci* [2006] EWHC 1442 (Ch)
[858] eg, in *British Telecommunications Plc v One In A Million Ltd* [1999] 1 WLR 903 *and Global v Citigroup* [2005] EWHC 2663 (Ch)
[859] **n858**; followed in *Bonnier Media Ltd v Smith* 2002 SCLR 977
[860] **n858**. Here it was held that mere registration and forceful maintenance of a usurped domain name made that domain name a potential instrument of fraud.

these cases like others preceding them, courts demonstrate a preference for using passing off rather than trademark law to protect domain names.[861]

5.2.5.2.2. India

The law of trademarks (vis a vis the Trademarks Act 1999, as amended) regulates domain names in India. There have been a number of judgments by different high courts on the subject[862] holding that legitimate domain name holders are entitled to protection akin to trademark owners.[863]

It can be concluded here that the law of trademarks and passing off are both used to regulate domain names in the UK and India.

5.2.5.3.Passing off

The law of Passing Off, as already evident in the case of domain names, regulates digital identity. This section examines its broader applicability.

5.2.5.3.1. UK

Passing off[864] developed in English common law and was adopted by Scotland and India. It was defined by the House of Lords in *Reckitt and Coleman Products v Borden Inc*[865] in terms of the elements that were necessary for a party to bring a successful passing off action: goodwill in goods or services, a misrepresentation likely to deceive and damage suffered or likely to be suffered. This was extended after *Bollinger v Costa Brava Wire Co,*[866] in *Erven Warnink v Townend*[867] to include that fact of misrepresentation was made in the course of trade by a trader to

[861] *Glaxo v Glaxowellcome Limited* [1996] FSR 388; *Direct Line Group Limited v Direct Line Estate Agency Limited* [1997] FSR 374; *Easyjet Airline Co v Tim Dainty* [2002] FSR 6
[862] *Tata Sons Ltd. v Manu Kosuri* 2001 PTC 432 (Del), *Dr. Reddy's Laboratories Ltd. v Manu Kosuri* 2001 PTC 859 (Del), *Acqua Minerals Ltd. v Shailesh Gupta* 2002 (24) PTC 35.5 (Del), *Microsoft Corporation v Deepak Chandwani*, Unreported ex parte interim injunction order, Suit 1680/99 (Del)
[863] See *Yahoo! Inc v Akash Arora & Anr* 1999 PTC (19) 201, *Rediff Communication Ltd v Cyberbooth* 1999 (3) All MR 164 (Bom), *DM Entertainment v Jhaveri,* Case 1147/2001 (Del)
[864] Preferred choice of law in cybersquatting disputes.
[865] [1990] RPC 341
[866] [1960] Ch 262
[867] [1979] AC 731, 742

prospective or ultimate consumers, calculated to injure another's goodwill or business and causes actual damage.[868]

Personal names that acquire secondary meaning through trade or business use may be protected under the law of passing off e.g. Johnny Walker,[869] John Haigh,[870] Thistle,[871] Charles Rennie Macintosh[872] and Alan Clark.[873] Business names are protected if distinctive. For example, Maxim's,[874] Dr Crock and his Crackpots,[875] The Drifters[876] etc. Distinctive abbreviations, letters and numerals have also been granted protection.[877] For instance, CA,[878] BMA,[879] 1001,[880] 4711.[881] It can safely be argued that this applies to digital names and numbers as well.

5.2.5.3.2. India

Passing off[882] finds statutory basis under Sections 27 (2), 134 (1) (c) and 135 of the Trade Marks Act 1999. Section 27 (2) provides that a person might have a right of action against another person for passing off goods or services as the goods of another person or as services provided by another person, or the remedies in respect thereof. Section 134 (1) (c) provides that no suit for passing off arising out of the use by the defendant of any trade mark which is identical with or deceptively similar to the plaintiffs trade mark, whether registered or unregistered, shall be instituted in any

[868] *Kean v McGivan* [1982] FSR 119
[869] *John Walker and Sons Ltd v Henry Ost & Co Ltd* [1970] RPC 489
[870] *John Haigh and Co Ltd v John DD Haigh Ltd* 1957 SLT (Notes) 36
[871] *Thistle v Thistle Telecom Ltd* 2000 SLT 262
[872] *Carrick Jewellery Ltd v Ortak* 1989 GWD 35-1624
[873] *Clark v Associated Newspapers* [1998] RPC 261
[874] *Maxim's Ltd v Dye* [1977] FSR 364
[875] *Hines v Winnick* [1947] Ch 708
[876] *Treadwell's Drifters Inc v RCL Ltd* 1996 SLT 1048
[877] Hector MacQueen, Charlotte Waelde, Graeme Laurie, Abbe Brown, *Contemporary Intellectual Property: Law and Policy* (OUP, Oxford 2010), 728
[878] *Society of Accountants in Edinburgh v Corporation of Accountants* (1893) 20R 750
[879] *British Medical Association v Marsh* (1931) 48 RPC 565
[880] *PC Products v Dalton* [1957] RPC 199
[881] *Reuter v Muhlens* (1953) 70 RPC 235
[882] For detailed analysis, see P Narayanan, *Law of Trade Marks and Passing Off* (Eastern Law House, New Delhi 2004), 520, Justice VA Mohta, *Trade Marks, Passing Off and Franchising* (All India Reporter, India 2004)

court inferior to a District Court having jurisdiction to try the suit. Section 135 deals with the reliefs available in passing off suits.[883]

The crux of passing off, stated in the case of *Ellora Industries v Banarsidas Goel,*[884] is "a cause of action arising out of confusion about the origin or source of a personal name, trade name or mark.[885] In *NR Dongre v Whirlpool Corporation*,[886] the Supreme Court while upholding an injunction obtained in respect of passing off, held that where there goodwill and reputation is acquired in respect with a mark, there inheres a right to protect against the invasion of that mark.[887]

Passing off is available to protect trade names, symbols, signs, devices and unregistered trademarks. But passing off actions are not just limited to protecting goods and services in the course of trade, and can be extended to other fields of activity.[888] Thus, it has a wider scope than the law of trademarks. Moreover, it is not just national reputation and goodwill that is protected by passing off actions.[889]
A digital identity will be protected against harm to its reputation and goodwill if any passing off in respect of it is found to exist (what would be required to be proven is deceptive similarity and confusion,[890] misrepresentation and loss or damage of goodwill).[891] Passing off has been held to be available to owners of distinctive domain names in cases of their infringement. [892]

---

[883] These are: injunction (subject to such terms, if any, as the court thinks fit) and at the option of the plaintiff, either damages or an account of profits, together with or without any order for the delivery-up of the infringement labels and marks for destruction or erasure - S 135 (1)
[884] AIR 1980 Del 254
[885] Para 33
[886] (1996) 5 SCC 714
[887] Para 10. It further stated that "a man is not to sell his own goods under the pretence that they are the goods of another man."
[888] VV Sople, *Managing Intellectual Property: The Strategic Imperative* (Prentice-Hall, New Delhi 2006), 113
[889] *Mars Incorporated v Chanda Softy Ice Cream* AIR 2001 Madras 237; *Intel Corporation v S Ramanan* 2002 (25) PTC 457 Mad
[890] See *Cadila Health Care Ltd v Cadila Pharmaceuticals Ltd.* (2001) SCL 534; *Kishore Zarda Factory (P) Ltd v JP Tobacco House* AIR 1999 Delhi 172, 175; *Kirloskar Proprietary Ltd v Kirloskar Dimensions* AIR 1997 Karnataka 1; *Roshan Lal Oil Mills Ltd v Assam Co Ltd* 1996 (16) PTC 699
[891] *Hindustan Radiators Co v Hindustan Radiators Ltd* AIR 1987 Del 353; *Athletes Foot Marketing Adm Inc v Cobra Sports Limited* 1980 RPC 343
[892] *Satyam Infoway Ltd v Sifynet Solutions* CA 028/2004 (Supreme Court), *Titan Industries Ltd v Prashant Koapati,* Interloc Interim App 787/1998, CS 179/1998 (Delhi High Court).

Again, in both the case of UK and India one finds grounds of similarity in the letter of passing off law and the requirements it would impose for digital identity to be protected under its ambit.

5.2.5.4.Copyright

Copyright law also regulates digital identity. Copyright is defined as "a legal term describing rights given to creators for their literary and artistic works."[893] Copyright is a bundle of limited term rights in relation to original and expressed works of literary or artistic nature (dramatic works, sound recordings). Rights under copyright accrue to the copyright holder and are used to prevent certain acts (e.g. reproduction, public performance, recording, broadcasting or translation) in respect of copyrighted work unless authorised.

Digital identity would qualify for copyright protection if it fell within the scope of protected works under copyright law. For instance, copyright might protect original email and blog content. It could be used to protect a digital performances (through performers' rights), digital images, paintings, illustrations and photographs, digital characters like MMORPG ids and Avatars.

To protect digital identity expression, holders of copyright in such identities often resort to the use of technological tools to prevent their digital identities being infringed. This is done through the use of tools like digital watermarking, fingerprinting, encryption (e.g. content scrambling). The law supports the use of these tools and in many cases, outlaws the use of measures that circumvent these technologies.

International copyright law is embodied in treaties like: the Berne Convention for the Protection of Literary and Artistic Works,[894] the Brussels Convention Relating to the Distribution of Program-Carrying Signals Transmitted by Satellite,[895] Convention for the Protection of Producers of Phonograms against Unauthorized Duplication of

[893] WIPO, 'Copyright and Related Rights, What is Copyright?'<http://www.wipo.int/about-ip/en/copyright.html>
[894] In force both in UK and India.
[895] Neither UK nor India is party.

Their Phonograms,[896] Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations.[897] Some copyright provisions can also be found in the TRIPS Agreement. [898]

In addition, the Internet treaties - the WIPO Copyright Treaty (WCT)[899] and the WIPO Performances and Phonograms Treaty (WPPT)[900]- expand the protection of copyright to works disseminated over the Internet and other digital technologies. Countries, however, have some element of freedom in setting forth what exceptions and limitations exist in respect of the rights granted by these treaties. While the UK is a contracting party to both treaties,[901] India is not.

5.2.5.4.1. UK

The Copyright, Designs and Patents Act 1988 (CDPA 1988), as amended in October 2003 by the Copyright and Related Rights Regulations 2003,[902] forms the current framework of copyright law in the UK.[903] The basis of copyright protection was summed up in *LB (Plastics) Ltd v Swish Products Ltd*[904] which stated that "one man must not be able to appropriate the result of another's labour."

Copyright law in the UK protects literary works (any work, other than a dramatic or musical work, which is written, spoken or sung and that includes a table or compilation, a computer program,[905] preparatory design material for a computer program and a database[906]), dramatic works (work of dance or mime), musical works (work consisting of music, exclusive of any words or action intended to be sung,

[896] In force both in UK and India.
[897] In force in the UK; only signed by India.
[898] Part II, S 1 of the Agreement deals with copyright and related rights
[899] Adopted in Geneva on 20 December 1996
[900] Adopted in Geneva on 20 December 1996
[901] The WCT and WPPT were signed by the UK on 13 February 1997, ratified on 14 December 2009 and entered into force from 14 March 2010.
[902] Incorporating the changes mandated by the Information Society Directive.
[903] Copyright law finds its origins in common law in the Statute of Anne and became statutory post the Copyright Act 1911.
[904] [1977] FSPLR 87. In line with *Walter v Lane* (1990) AC 539 and *Ravencroft v Herbert* (1980) RPC 103
[905] Included by the Copyright (Computer Programs) Regulations 1992
[906] Database, per the CDPA 1988 S 3(A), refers to a collection of independent works, data or other materials which are arranged in a systematic or methodical way, are individually accessible by electronic or other means and is an original intellectual creation of the author.

spoken or performed with the music), artistic works (includes graphic work, photograph, sculpture or collage, irrespective of artistic quality, works of architecture, and works of artistic craftsmanship),[907] typographical arrangements of publications, sound recordings,[908] films and broadcasts (electronic transmission of visual images).[909]

Copyright automatically accrues to the author (or producer or commissioner, depending on context) of a work. The duration of copyright varies depending on the nature of the work.[910] The rights that vest in the holder of a copyright are: right to copy the work,[911] to issue copies of the work to the public,[912] to rent or lend the work to the public,[913] to perform, show or play the work in public,[914] to communicate the work to the public,[915] to make an adaptation of the work or do any of the above in relation to an adaptation[916] and a right to do any of the acts restricted by the copyright.

Infringement of copyright occurs when works restricted from being copied, are copied.[917] Copying can take the form of reproducing work in material form or storing it on any medium by electronic means, making different dimensional copies, making photographs of whole or substantial parts of films, making facsimile copies, or even the making of transient or incidental copies.[918] Infringement by copying can also occur by issue of copies to the public,[919] by rental or lending of work to the public,[920]

---

[907] CDPA 1988, S 4 (1)
[908] S 5A
[909] CDPA 1988, S 1
[910] Duration is prescribed in Ch I, ss 12-14, CDPA 1988, and ranges from 25-70 years.
[911] S 17
[912] S 18
[913] S 18A
[914] S 19
[915] S 20
[916] S 21
[917] S 17
[918] S 17
[919] S 18
[920] S 18A

by performance, showing or playing of work in public,[921] by communication to the public,[922] or by making adaptation or act done in relation to adaptation.[923]

All acts in respect of copyrighted works are not restricted. Certain acts are permitted in relation to copyright works:[924] fair dealing in respect of research and private study,[925] fair dealing for criticism, review and news reporting,[926] incidental non-deliberate inclusion of copyright material,[927] making of a single accessible copy for personal use,[928] or multiple copies in relation to visual impairment problems.[929]

The CDPA 1988 provides various remedies for infringement of copyright[930] actionable by the copyright owner.[931] These remedies include damages, injunctions, accounts and any such relief as is otherwise available in respect of the infringement of any other property right.[932] There are also some criminal provisions.[933]

Thus a digital identity would be protected under copyright law in the UK if copyright subsisted in it.

5.2.5.4.2. India

In India,[934] the current legal framework is represented by the Copyright Act 1957[935] (as amended by the Copyright (Amendment) Act 1999).[936] Copyright is visualised as

---

[921] S 19
[922] S 20
[923] S 21
[924] Prescribed in Ch III, CDPA 1988 (full list available there)
[925] S 29
[926] S 30
[927] S 31
[928] S 31A
[929] S 31B
[930] Ch VI
[931] S 96 (1)
[932] S 96 (2)
[933] S 107 deals with criminal liability for making or dealing with infringing articles.
[934] India is a party to the Berne Convention for Protection of Literary and Artistic Works (1886) and the Universal Copyright Convention.
[935] The 1957 Indian Act was largely influenced by the UK Copyright Act of 1956 and has been amended several times (1983, 1984, 1992, 1994 and 1999). The 1994 amendment is the most significant because it harmonised the Act with the 1961 Rome Convention by providing protection to performers' rights, producers of phonograms and broadcasting organisations and introduced registration of Copyright Societies.

a bundle of rights, of economic and moral nature, that accrue to the holder of the copyright.

Copyright, under Indian law, exists in the following works: [937] original literary works,[938] dramatic works,[939] musical works[940] and artistic works like paintings, sculpture, drawing (including diagrams, maps, charts or plans), engravings or photographs,[941] whether or not any such work possesses artistic quality, work of architecture[942] and work of artistic craftsmanship,[943] cinematograph films[944] and sound recordings.[945]

The nature of rights under copyright is clarified by section 14 of the Act. These include: rights reproducing, storing, selling or hiring out works, making and issuing copies of works, performing or communicating works, making recordings, translations or adaptations, or offering commercial rentals.[946] The duration of copyright is prescribed in Chapter V of the Act.[947]

Not all acts done in respect of copyright material would constitute an infringement. The Copyright Act 1957 provides an extensive list of permitted acts in section 52 e.g. fair dealing for private use, research, criticism, review or news reporting, lawful making of copies in respect of certain permitted acts, the reproduction of a literary, dramatic, musical or artistic work for the purpose of a judicial proceeding or for the purpose of a report of a judicial proceeding, educational performances of copyrighted works, the licensed (or consent based) making of sound recordings in respect of any

---

[936] The Copyright (Amendment) Bill 2010 has been introduced in the Rajya Sabha to further amend the Copyright Act 1957. See <http://copyright.gov.in/Documents/CopyrightAmendmentBill2010.pdf> The Bill makes provisions for technological protection measures (S 65A) and rights management information (S 65B).
[937] S 13, Copyright Act 1957
[938] S 2 (o)
[939] S 2 (h)
[940] S 2 (p)
[941] S 2 (s)
[942] A building or structure having an artistic character or design, or any model for such building or structure. S 2 (b)
[943] S 2(c)
[944] Defined in s 2(f)
[945] Defined in s 2(xx)
[946] See s 14 for details.
[947] Ss 22-29. Generally 60 years.

literary dramatic or musical work; public airing of a recording in an enclosed non-commercial residential room or non-profit club, society or organisation etc.[948]

The Copyright Act imposes both civil (injunction, damages, accounts)[949] and criminal remedies (imprisonment and fines)[950] in respect of copyright infringement.

Thus, both countries have copyright law that, according to its own mandate, regulate the exercise of copyrighted digital identity.

5.2.5.5.Law of confidence

The law of confidence has also been used to protect personal information, which is an important form of digital identity. Intellectual property texts, both in the UK and India, classify the law of confidence as a class of intellectual property law[951] and this thesis maintains this trend.

The law of confidence would govern the relationship between digital identity subjects and digital identity controllers or managers, much in the manner that the data controllers or data processors may owe the data subject a duty of maintaining the confidentiality of information received in circumstances that obligate a condition of confidentiality.

5.2.5.5.1. UK

The precise "legal nature of breach of confidence actions in the UK is unclear"[952] with different arguments being put forth making the case that such actions are property actions (bolstered by the 'information as property' view) based on contract, English equity[953] or the Scots *actio in iniuriam* cause of action.[954] Personal

[948] For complete list see S 52 (a) - (za) of the Act.
[949] Chapter XII
[950] Chapter XIII
[951] UK: MacQueen,Waelde (2010) **n877**; Paul Torremans, *Hollyoak and Torremans: Intellectual Property Law,* (2005); India: P Narayanan, *Intellectual Property Law* (Eastern Law House, India 2004)
[952] MacQueen, Waelde (2010) **n877**, 768
[953] Not applicable in Scotland.

information embodied in private diaries or sexual activities,[955] residential details, domestic arrangements, photographs (of exposed bodies[956] and weddings[957]) have been actioned under breach of confidence.[958]

The law of confidence was invoked in the UK to protect the identity of the author of a blog in *The Author of a Blog v Times Newspapers Ltd*.[959] The author of the 'Night Jack' blog unsuccessfully sought an interim injunction to restrain Times Newspapers Ltd from publishing information that would identify him as the author of the blog. Eady LJ clarified that just the blogger's desire to maintain his anonymity did not signify either that he had a reasonable expectation of being able to do so or that the Times Newspaper was under any legal obligation to him in that respect.[960]

Eady LJ stated that blogging was a public, not private activity, and because of the nature of what the blogger wrote (material that was "political and highly critical of central and local policing strategies"), the public was entitled to know his identity so as to be able to assess and judge the value of the blog posts. It was concluded, by applying *Coco v AN Clark (Engineers) Ltd,*[961] that the identity of the blogger had "neither the necessary quality of confidence" nor did it qualify as anything that the blogger was capable of claming a reasonable expectation of privacy in. This case sets the remit of how digital identity might be regulated under the law of confidence in respect of the Internet. If a digital identity had the necessary quality of confidence about it, it would be protected under UK law.

---

[954] See HL MacQueen, 'Searching for Privacy in a Mixed Jurisdiction,' (2006) 21 Tulane European and Civil Law Forum, 73

[955] *Argyll v Argyll* [1967] Ch 302; *X (HA) v Y* [1988] 2 All ER 648

[956] As in the cases of Amanda Holden and Sara Cox. See Nick Higham, 'Privacy Law Remains Confused,' *BBC News* (9 June 2003) <http://news.bbc.co.uk/1/hi/uk/2975718.stm>

[957] *Douglas v Hello!* [2005] EWCA CIV 595, [2005] All ER (D) 280(May)

[958] UK courts assessment of breach of confidence actions takes into account Arts 8 & 10 of the ECHR and the HRA 1998.

[959] [2009] EWHC 1358 (QB)

[960] Referring to the comments of Toulson, LJ in *Napier v Pressdram Ltd* [2009] EWCA Civ 443 at [42]

[961] [1969] RPC 41. In *Coco v Clark,* a three step test was laid out: the information had to be confidential in nature, communicated in circumstances implying confidence and there had to be unauthorized use of the information to the detriment of the person making the confidence.

5.2.5.5.2. India

In India too, confidential information is protected from unauthorised use through breach of confidence remedies. Breach of confidence actions in India are based on the principle of equity (information received in confidence must not be unfairly used without consent, such that it prejudices the information giver or puts him at a disadvantage).[962] However, this tort has largely been used to protect information of commercial value and where some form of contractual relationship exists between parties.[963]

In the digital context, the duty of confidentiality is specifically, although rather inadequately embedded in Sections 72 and 72A of the ITA 2000. Section 72 prescribes a penalty for breach if any person securing access under the Act makes an unauthorised disclosure (of any electronic record, book, register, correspondence, information, document or other material) without consent.[964] The penalty prescribed is imprisonment of up to two years or fine extending to one lakh rupees or both.

Section 72A which deals with disclosure of information in breach of lawful contract, states,

> any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

However, as this provision only applies in cases where there is a lawful contract between two parties, it does not cover cases where individuals find the confidentiality of their personal information breached by other individuals or entities

[962] Equitable obligations exist even out with contract.
[963] Eg, *Zee Telefilms v Sundial Communications* 2003(5) BomCR 404, *Diljeet Titus v Alfred Adebare* 130 (2006) DLT 330, *UJ Chiang v Global Broadcast News* 2008 (2) BomCR 400, *John Richard Brady v Chemical Process Equipments* AIR 1987 Delhi 372, *Michael HN Johnson v Subhash Chandra* 60 (1995) DLT 757
[964] N Salim, 'Breach of Privacy and Confidentiality Under Information Technology Act, 2000' *Legal Service India* (10 January 2009) <http://www.legalserviceindia.com/article/l288-Breach-of-privacy-&-Confidentiality-.html>

that they do not share contractual relations with. Thus, the confidentiality of digital identity of individuals is not well protected under this regime; and though it could be argued that the general law of confidence could be brought to apply to protect the confidentiality of digital identity of individuals, there is no evidence to support that this has or will be the future direction that the law will take.

In the case of the law of confidence, a divergence between the UK and Indian legal positions is evident. While a trend of protecting personal information is evident in the UK context, no such trend is evident in India.

5.2.6. Tort law

Torts are civil wrongs actioned by one person against another in a court of law. The principle underlying tort law is '*ubi jus ibi remedium*,' i.e. where there is right there is a remedy.

The Law of Torts relates to digital identities and protects them in cases where such identities have been wronged in the manner prescribed by such law. There are many examples of digital identity torts, primary among which are: defamation,[965] negligence, malicious falsehood and misuse of private information. *Tortum*[966] or *jimha*[967] acts in respect of a digital identity would, all conditions fulfilling, give rise actions for *remedium* (remedy, largely in the form of damages).Tort law has been employed to protect facets of digital identity elsewhere in the world e.g. Australia,[968] France[969] and the US.[970]

[965] Defamation is probably the most prevalent tort used in the digital identity context, which demonstrates the significance attached to reputation and its defense against tarnishment or vilification.
[966] Latin for twisted or crooked.
[967] The Sanskrit term for tort. P Sen, *The General Principles of Hindu Jurisprudence* (Saraswat Library, Calcutta 1918), 211.
[968] See *Rindos v Hardwick,* Supreme Court of Western Australia, (unreported), 31 March 1994, (defamation), *The Buddhist Society of Western Australia Inc v Bristile Ltd & Anor* [2000] WASCA 210 (9 August 2000) (defamation), *Gutnick v Dow Jones & Co Inc* [2001] VSC 305 (28 August 2001) (defamation), *Cullen v White* (2003) WASC 153) (defamation, ID crime*), Adam Kaplan v Go Daddy Group Inc* [2005] NSWSC 636 (tort of injurious falsehood)
[969] *Lefebure v Lacambre,* 55181/98, No. 1/JP (defamation, privacy and personality rights)
[970] Successfully in some cases, unsuccessfully in others. *Cubby, Inc v CompuServe Inc* 776 F. Supp. 135 (SDNY 1991) (defamation); *Lunney v Prodigy Servs. Co* 683 NYS2d 557, NY App, 2d Div. 1998 (defamation); *Stratton Oakmont v Prodigy* NY Sup Ct 1995 (defamation); *Barrett v Fonorow* 112 Cal App 4th 749 (2003) (defamation)*; Barrett v Rosenthal*112 Cal App 4th 749 (2003) (defamation); *Kremen v Cohen* 337 F 3d 1024 (9th Cir 2003) (conversion of Internet domain name); *Scheff v Bock* Case No 3022837, Circuit Court, Broward County, Florida (defamation)

England has the law of torts, while Scotland has the Law of Delict (or Delictual Liability).[971] The Indian Law of Torts was influenced by English law and is adapted to suit local conditions.[972] It is an uncodified branch of civil law though it has been read into/aligned with other branches of law like criminal law[973] and constitutional law. This section examines elements of tort law that apply digital identity: defamation, malicious falsehood, negligence and misuse of private information.

5.2.6.1.Defamation

Actions for defamation are commonplace in the protection of digital reputation. This section examines how this tort has been invoked in relation to and regulates digital identity.

5.2.6.1.1. UK

The law of defamation in the UK finds basis in common law and the Defamation Acts of 1952 and 1996. By nature, defamation is a civil tort.

Tort law has been invoked and successfully applied in a number of cases in the UK, particularly in relation to Internet based defamation. For example, *Godfrey v Demon Internet*[974] *Loutchansky v Times Newspapers,*[975] *Totalise Plc v Motley Fool*,[976] *Jim Murray v Jonathan Spencer*,[977] *Robertson v Newsquest*,[978] *Keith-Smith v Williams*,[979] *Applause Store Productions Ltd and Firsht v Raphael*[980] and *Metropolitan International Schools Ltd v Designtechnica Corporation and Others.*[981]

---

[971] For overview, see DM Walker, *The Law of Delict in Scotland* (Sweet & Maxwell, Edinburgh 1981)
[972] R Ratanlal and KT Dhirajlal, *The Law of Torts* (Wadhwa, Nagpur 2004),1-2; MC Setalvad, *The Common Law in India* (Hamlyn Trust, 1960), 110; See the opinion of Justice Krishna Aiyar in on the tort of conspiracy in *Rohtas Industries Ltd. v Rohtas Industries Staff Union,* AIR 1976 SC 425 and comments of Justice Bhagwati in *MC Mehta v Union of India* AIR 1988 SC 1037
[973] Defamatory torts like libel and slander are also criminal offences. See s 499, IPC.
[974] **n188**
[975] [2001] EWCA Civ 536 (Internet libel)
[976] [2001] EWCA Civ 1897 (Internet libel, Norwich Pharmacol Application)
[977] 20 May 2002, Lincoln County Court (Internet libel)
[978] 2006 SCLR 792 (repetitive libel)
[979] [2006] EWHC 860 (QB) (successful Internet libel case between two individuals.
[980] [2008] EWHC 1781 (QB) (Internet libel/suit between friends regarding creation of false Facebook profile)
[981] [2009] EWHC 1765 (QB) (non-human conveyor of defamatory material cannot be held liable for defamation)

5.2.6.1.2. India

In India, there are few instances of the tort of defamation being used to deal with Internet defamation, as evident in the following cases: *SMC Pneumatics (India) Pvt. Ltd. v Jogesh Kwatra,*[982] *Gremach Infrastructure Equipments & Projects Limited* v *Google India Private Limited*[983] and *Socieadade de Fomento Industrial Pvt Ltd v Sebastian (Sebi) Rodrigues.*[984] All these cases again are cases in which commercial reputation has been protected from misuse.

Defamation is both a crime and a tort in India. Criminal law of defamation is more widely established and employed in cases of alleged Internet defamation in relation to protection of individual reputation vis a vis other individuals.[985]

In respect of the law of defamation, are evident vast differences in the law of the UK and India.

5.2.6.2.Malicious falsehood

Malicious falsehood implies the making of some malicious false statements or allegations or remarks. The tort of malicious falsehood has a wider ambit than the tort of defamation and would apply to digital identity. In an action for malicious falsehood, there is no need to show loss of reputation for the recovery of damages.

5.2.6.2.1. UK

Malicious falsehood, per Harpwood, is the "publication of disparaging remarks about a person's goods or services."[986] But, this tort[987] though largely used to protect business interests, may also be used to protect personal reputation.[988] There are generally three elements required to prove this tort: publication, malice and actual

[982] CS 1279/2001 (Del). Unreported. Injunction retraining publication granted.
[983] CS 506/2008, 18 Feb 2008 (Bom). Ad interim order of injunction granted and order for disclosure of blogger identity made.
[984] CS 265/2008 (Kol). Interim order of injunction granted on 2 September 2009.
[985] See further **Ch 6, 6.3.3**
[986] V Harpwood, *Principles of Tort Law* (Routledge, UK 2000), 401
[987] In England, one can get legal aid for the tort of malicious falsehood, unlike defamation. Damages in respect of malicious falsehood are lesser as compared to defamation.
[988] See *Joyce v Sengupta* [1993] 1 All ER 897

loss.[989] Malice is inferred if the words used in making the allegation are either intended to produce some damage and there was some recklessness on the part of the maker of the statement as to its veracity.[990]

5.2.6.2.2. India

In India, the tort of injurious or malicious falsehood "relates to those statements which are false but not defamatory and which do not constitute either slander of goods or slander of title. For a successful claim of malicious falsehood, a claimant must prove:

(i) A false statement calculated to cause financial damage was made[991]
(ii) The statement was made maliciously with intent to cause injury,
(iii) The statement has resulted in a special damage unlike in defamation in which the falsehood of the statement is presumed, and it is for the defendant to prove that the statement is true.[992]

The tort of malicious falsehood would apply in both UK and India to protect digital identities, if the prescribed conditions are fulfilled.

5.2.6.3.Negligence

The tort of negligence is a substantial part of tort law. It occurs if a person breaches a duty of care owed to another and the breach causes loss to the person the duty is owed to. The nature of the duty was laid down in the famous case of *Donoghue v Stevenson.*[993] Lord Atkin stated, "You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour." If a duty of care and its breach is established, a claimant must also show that loss has been suffered and quantify that loss.

The tort of negligence applies in the regulation of digital identity. For instance, a digital identity could be classed as a product[994] and liability would arise in respect of a breach of a duty of care owed in respect of it. An identity management or service

[989] Where the truth of the claim or malice was not proved, the case failed. *Christopher John Quinton v Robin H Peirce* [2009] EWHC 912 (QB).
[990] *Kaye v Robertson* [1991] FSR 62 (CA)
[991] *Manisha Koirala v Shashilal Nair* 2003 (2) BomCR 136
[992] *Dabur India Ltd v M/S Colortek Meghalaya Pvt Ltd* CS(OS) 2029/2009 (Del)
[993] [1932] AC 562,580
[994] S Hedley, *Tort* (OUP, Oxford 2006), 91

provider might owe a duty of care to a digital identity subject. If that duty of care is breached, and loss is caused to the digital identity subject, then the digital identity subject could make a claim under the tort of negligence against that identity management or service provider.

Negligence has been invoked in respect of digital identity in a number of US cases: *Marsha L Shames-Yeakel v Citizens Financial Bank*,[995] *Jones v Commerce Bancorp, Inc.*, No. 06[996] *Bell v Mich. Council 25 of Am. Federation of State, County, Municipal Employees*.[997] In these cases, it was recognised that there was a common law duty on financial institutions to safeguard members and customers confidential information from identity fraud.

5.2.6.3.1. UK

In England, the tort of negligence has three elements: a duty of care,[998] a breach in respect of a duty owed[999] and consequent damage.[1000] The nature of tort law here is to provide a remedy where an injury or loss results from the failure to maintain a legal duty of reasonable care.[1001] To understand how this would apply in the digital context, let's take an example. Under the DPA 1998, data controllers are obligated to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.[1002] Where there is a failure to meet this obligation through breach of a duty of care and damage results, an action of negligence would arise.

[995] USDC, Northern District of Illinois, Case No. 07-c-5387, 21 August 2009
[996] Civ 835, 2006 WL 1409492, at *2 (SDNY, 23 May 2006)
[997] No. 246684, 2005 WL 356306, at *1 (Mich Ct App, 15 February 2005) (per curiam)
[998] For scope of the duty of care see *Bourhill v Young* [1943] AC 92; *Palsgraf v Long Island Railroad Co* (1928) 248 NY 339; *Haley v London Electricity Board* [1965] AC 778: *Urbanski v Patel* (1978) 84 DLR (3rd) 650; *Goodwill v British Pregnancy Advisory Service* [1996] 2 All ER 161
[999] *Blythe v Birmingham Waterworks* (1856) 11 Exch 781
[1000] *Lochgelly Iron and Coal Co v McMullan* [1934] AC 1 at 25
[1001] For comprehensive coverage of the tort of negligence, see Vivienne Harpwood, *Modern Tort Law,* (Cavendish Publishing, London 2005), 19-26
[1002] Seventh Data Protection Principle, Schedule 1, Part I, (7)

5.2.6.3.2. India

In India too, the tort of negligence[1003] affords action where there is a breach of duty of care[1004] and injury results.[1005] For example, if it can be shown that a company or association failed to implement and maintain reasonable security practices and procedures in respect of data or information of an individual, and a wrongful loss or wrongful gain is caused to that individual, that individual could bring an action for negligence.[1006]

5.2.6.4.Misuse of private information

The misuse of private information (and consequently digital identity constituting private information) may also be actioned under tort law.[1007]

5.2.6.4.1. UK

In *Cambell v MGN*,[1008] Lord Nicholls expressed the independent existence of a limited tort[1009] of misuse of private information (free from the limiting constraints of breach of confidence actions).[1010] This tort "affords respect for one aspect of an individual's privacy."[1011] This tort however, only protects private information one has a reasonable expectation of privacy in.[1012]

[1003] Scope examined by the Supreme Court in *Rajkot Municipal Corporation* v *Manjulben Nakum* (1997) 9 SCC 552.
[1004] *Klaus Mittelbachert v East India Hotels Ltd* AIR 1997 Del 201.
[1005] *Spring Meadows Hospital v Harjot Ahluwalia* (1998) 4 SCC 39, *Mrs. Shanta v State of AP* AIR 1998 AP 51, *RSEB v Jai Singh* AIR 1997 Raj 141; *AS Zingthan v State of Manipur* AIR 1998 Gau 102.
[1006] However, no case law was found on tort of negligence being used to protect personal data or sensitive personal data.
[1007] For a detailed analysis of why the tort of misuse of information must be treated separately to breach of confidence, see John Murphy, *Street on Torts* (OUP, Oxford 2007), 385-394
[1008] [2004] UKHL 22
[1009] Not all privacy violations are actionable under the tort and they would be judged in the light of Arts 8 and 10 of the ECHR. See NJ McBride, R Bagshaw, *Tort Law* (Pearson Education, Edinburgh 2008), 319-341
[1010] Paras 12-15
[1011] Lord Nicholls, para 15
[1012] *Cambell v MGN,* paras 21 and 85

5.2.6.4.2. India

Though the law affords a general and consequential tort remedy (i.e. damages) for the unlawful invasion of privacy,[1013] it does not offer parallel protection as evidenced in the case of the UK to the misuse of private information.

In summary, tort law in the UK would generally apply to digital identity a manner not much different from how it would in India. Yet, there are also distinctions in its application as evident in the nature and use of the law of defamation and the use of tort law to protect private information.

5.2.7. Data protection law

Data protection law affects digital identity immensely, particularly in Europe.[1014] The EU has a well developed data protection regime embodied in the following legislative instruments and provisions:

1. The ECHR, specifically Article 8. [1015]
2. Treaty on the European Union [1016]
3. The Data Protection Directive.[1017]
4. The Telecommunications Data Protection Directive.[1018]
5. Charter of the Fundamental Rights of the European Union, notably Article 8 on the protection of personal data.[1019]
6. Directive on Privacy and Electronic Communications[1020]
7. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC[1021]

In Europe generally, prevalent privacy and data protection culture and regulation has resulted in digital identity becoming enmeshed and inextricably linked to *personal*

[1013] *Rajagopal* **n722** § 9
[1014] Data protection here refers to the protection of personal data or information, distinct from privacy.
[1015] Data protection law in Europe is also influenced by international human rights instruments like the UDHR and the ICCPR. Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits,* (Kluwer Law International, The Hague 2002), 116
[1016] Consolidated version at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:EN:PDF>
[1017] Directive 95/46/EC
[1018] Directive 97/66/EC
[1019] see **n579**
[1020] Directive 2002/58/EC
[1021] [2006] OJ L 105/54

data[1022] as demonstrated in Chapter 2.[1023] This is of particular importance to us, because many of the digital identity manifestations are brought under the purview of data protection law and also because data protection law fundamentally exists to protect individuals in Europe against the violation of their various fundamental rights.[1024] It also regulates the behaviour of two important actors in the digital identity network - the data controller and the data subject.[1025]

Contemporary data protection law enables digital identity subjects in Europe to control the collection, storage, processing, use and dissemination of their personal information. The Data Protection Directive sets out substantial requirements in this respect. Forming the crux is Article 6 of the Directive which sets out the data protection principles in relation to personal data: fair and lawful processing, purpose limitation, data adequacy, accuracy of data, time limitation). Other significant elements are: data subject's right of access to data (Article 12a), integrity of data (Article 12b), automated decision making (Article 15), security of data (Article 17) and conditions of transfer of data to third countries (Chapter IV). These principles, it has been argued, generally apply to digital identity.[1026]

5.2.7.1.UK

Data protection law is well established in the UK. Currently, the DPA 1998,[1027] together with other statutory instruments,[1028] sets out the legal regime for data protection in the UK and aims at regulating the "processing of information relating to

---

[1022] Article 2 (a); *Bodil Lindqvist* [2004] 1 CMLR 20
[1023] **2.4.3**
[1024] See Recitals of the Directive.
[1025] Note this includes protection only for natural persons. Austria, Denmark, Italy and Luxembourg have extended their data protection laws to legal persons. D Korff, 'Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons,' (February 2001) <http://europa.eu.int/comm/internal_market/privacy/studies/legal_en.htm>
[1026] T Olsen and T Mahler, 'Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust' Part II,' (2007) 23 CLSR, 415-426
[1027] Repealed the Data Protection Act 1984.
[1028] Eg, The Data Protection Act 1998 (Commencement) Order 2000, The Data Protection Tribunal (National Security Appeals) (Telecommunications) Rules 2000; The Data Protection (Processing of Sensitive Personal Data) Order 2000, The Privacy and Electronic Communications (EC Directive) Regulations 2003, The Information Tribunal (Enforcement Appeals) Rules 2005, The Information Tribunal (Enforcement Appeals) (Amendment) Rules 2005, The Information Tribunal (National Security Appeals) Rules 2005, The Data Protection (Processing of Sensitive Personal Data) Order 2006; The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010. For comprehensive list see Department of Constitutional Affairs, <http://www.dca.gov.uk/ccpd/dpsubleg.htm>

individuals, including the obtaining, holding, use or disclosure of such information."[1029] The DPA 1998 does not operate in isolation but is used in conjunction with the Freedom of Information Act 2000 (in Scotland, The Freedom of Information (Scotland) Act 2002).

In the UK, data protection law protects digital identities in the form of personal data. Personal data is data relating to a living individual who can be identified from that data or from data or other information possessed or likely to be possessed by a data controller.[1030] For instance, a digital name,[1031] a CCTV image or a social networking profile that can be connected to a living identifiable person.

In *Durant v FSA,*[1032] the Court of Appeal ruled on what comprised "personal data" and came up with two elements: one, identifiability of the individual from the information, and second, that the information related to the individual such that it impacted his/her privacy (in some way or the other). The UK Information Commissioner further clarified this and said that an individual's name was a key aspect of identity specifically where it coupled with other personal biographical information, and well within the purview of data protection law.[1033]

5.2.7.2.India

In India, unlike the UK, there is no specific and established data protection legal regime. There are no data protection principles (as evident in the European or UK regime) for data controllers and processors to follow that set the remit of what is permissible behaviour in respect of personal data, and consequently digital identity. However, the ITA 2000 (as amended by ITAA 2008) does contain some data protection provisions.

[1029] <http://www.opsi.gov.uk/Acts/acts1998/ukpga_19980029_en_2#pt1-l1g1>
[1030] S 1(1), DPA 1998
[1031] A name by itself may not constitute personal data. But names are rarely used by themselves, and often used in conjunction with other data that can lead to identification of a living individual.
[1032] [2003] EWCA Civ 1746
[1033] UK Information Commissioner, 'The "Durant" Case and its Impact on the Interpretation of the Data Protection Act 1998,' (27 February 2006) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf>

The first is the provision for compensation for failure to protect data embodied in section 43A.[1034] It provides that corporate bodies[1035] possessing, dealing or handling sensitive personal data[1036] or information in any of their owned, operated or controlled computer resources and negligently failing to implement and maintain reasonable security practices and procedures, which result in wrongful loss or gain, will be liable to pay compensatory damages.

The second is the data confidentiality provision in section 72A. It provides that a person while providing services under a lawful contract must not disclose personal information obtained during that contract. If such a disclosure occurs (without consent or in breach) and it causes wrongful gain or loss, a punishment or fine might result.

Both the above provisions give digital identity subjects a semblance of control over their information or data. But they are very limited in their application and effectiveness in protecting and securing digital identity (as also demonstrated in the following Chapter[1037]). Data protection law in India was largely influenced and incentivised by Europe's 'standard of reciprocity' under Articles 25 and 26 of the DPD.[1038]

Thus, data protection law in the two jurisdictions is very dissimilar. In the UK, it is highly advanced in nature and spirit; in India it is very nascent. Thus it places digital identity subjects in the two jurisdictions on unequal footing.

5.2.8. Taking stock

The examination of the law regulating digital identity in the UK and India provides unusual results. Given the diverse nature of the UK and Indian jurisdictions, and particularly local difference evident in relation to digital identity, it was expected that vast differences would emerge. However, there are a number of broad similarities in

[1034] Inserted by ITAA 2008
[1035] Includes any company including firm or sole trader or professional associations of individuals.
[1036] S 43A (iii)
[1037] See **6.3.4.1, 6.3.7.2**
[1038] See Bharat Vagadia, *Outsourcing to India: A Legal Handbook* (Springer, Berlin 2007), 123

the letter of the law in addition to significant differences. The similarities are evident in the context of criminal law, contract law, intellectual property law and some principles of tort law (malicious falsehood and negligence). These similarities exist because of the nature and manner in which these laws were created in India.

Much of Indian law has foreign origin. As Galanter comments, "contemporary Indian law is for the most part, palpably foreign in origin or inspiration and it notoriously incongruent with the attitudes and concerns of much of the population which lives under it."[1039] Indian law, in large part, is based and borrows heavily from English law and legal precedents, due to India's colonial history. It also borrows from other Western jurisdictions like the EU and the US and draws from international laws.

Indian criminal law, for instance, is of British origin. The IPC of 1860 was formulated by the British appointed first law commission chaired by Lord Macaulay. In its formulation it represented a "foreign system" or a "system formed without the slightest reference to India,"[1040] However, as previously demonstrated[1041] and will become clearer in the following chapter,[1042] this system of law (in current form), works well to regulate digital identity in India.

Indian contract law, as embodied in the Indian Contract Act 1872 is based on English common law.[1043] Therefore it is not surprising that it is similar to English contract law.

Intellectual property law in India has two natures – one, it was influenced by British law, and two, its internationally harmonised nature. The British influence is evident in the following examples. The Designs Act 1911 was passed under British rule. The Indian Patents Act 1970 was modelled on the UK Patents Act of 1949.[1044] The Indian

[1039] Marc Galanter, 'The Displacement of Traditional Law in Modern India' (1968) 24 (4) J of Soc Iss, 65-91
[1040] Sir George Pollock GCB, 'Report on the Indian Penal Code' (1850) 13, The Calcutta Review, 171
[1041] **5.2.1.2**
[1042] Specifically, **6.3.3**
[1043] Other statutes embodying English common law are the Evidence act 1872, the Transfer of Property Act 1882 (amended, 1929) and the Succession Act 1865. De Cruz (1999) **n281**, 175
[1044] Replaced by Patents Act 1977

Copyright Act 1957 was influenced by the UK Copyright Act of 1956. Passing Off is based upon common law and uses principles of English common law. India's intellecutal property law's harmonised nature has come about through India's acting to meet international legal obligations particularly under WTO TRIPS regime.

Indian tort law is also influenced by English law to a certain extent.[1045] This is evident in the context of law of negligence and malicious falsehood.

Even India's information technology law, primarily embodied in the ITA 2000 had a foreign thrust and influence to it. The Act was inspired and enacted to give effect to the UN Model Law on Electronic Commerce.[1046] Thus India consciously harmonised her law to meet international legal obligations. Though the ITA 2000 has been severely criticised,[1047] it continues (as amended in 2008) to function as the core basis for information technology regulation in India.

Thus, the Indian law regulating digital identity has much in common with the UK law and international law. A Westernised approach to digital identity regulation is palpable in the similarities. And yet, there are also significant differences. This is evident in relation to the regulation of privacy, the application of tort law (defamation and tort of misuse of private information) and data protection law.

5.2.9. Conclusion

The detailed comparative examination of the law regulating digital identity has brought out some significant results: first, digital identities occupy many "regulatory spaces."[1048] Second, there are a number of similarities in the law regulating digital identity. Third, there are significant differences in the law regulating digital identity.

[1045] See **5.2.6**

[1046] UN GA/RES/51/162, 30 Jan 1997

[1047] V Rajaraman, *Essentials of E-Commerce* (PHI, New Delhi 2010), 229; PT Joseph, *Ecommerce: An Indian Perspective* (PHI, India 2006), 28; SR Bhansali, *The Information Technology Act 2000: An Exhaustive, Critical and Analytical Commentary of Act No. 21 of 2000* (University Book House, 2003); Vivek Sood, *Cyberlaw Simplified* (Tata-McGraw Hill, India 2001), 5; Bagga (2005) **n290**, 145.

[1048] R Brownsword, 'So What Does the World Need Now? Reflections on Regulating Technologies,' in R Brownsword and K Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oxford 2008), 23-48, 30

These differences manifest themselves in the following respects: right to privacy, defamation, misuse of private information and data protection, some core areas of digital identity.

This chapter reveals on a broad and general level how the law regulates digital identity in the UK and India. But this is not the entire picture of how the legal regulation of digital identity occurs at national levels. How the law actually works in regulating digital identity is analysed next, with the help of specially formulated case studies on key aspects of digital identity.

6. The legal regulation of digital identity: Case studies

> …the future lies in 'diversity' and 'unity in diversity' rather than in unity through uniformity and standardisation.
> *-Esin Örücü*[1049]

6.1. Introduction

This chapter investigates in greater depth whether and how difference manifests in the legal regulation of digital identity in the UK and India from the applicatory perspective. This investigation is carried out with the help of case studies on principal aspects[1050] of digital identity like privacy, sharing, reputation, anonymity, pseudonymity, access to Internet resources and control of personal data (identified in the previous chapters as areas of local difference.)

6.2. Methodology

Case studies are a respected and potent form of legal education and research;[1051] a vital part of legal analysis and theory building[1052] and an essential demonstrative and learning tool. In this chapter, case studies function as an effective means to explore, gain insight into and demonstrate how the law operates to regulate digital identity in the UK and India.

These case studies examine digital identity regulation from a comparative perspective. A similar examination has not been conducted at the international level in this manner.[1053] In this respect, these case studies hope to become new food for thought for the legal and non-legal international and national digital identity

---

[1049] Esin Örücü, 'Comparatists and Extraordinary Places,' in Pierre Legrand and Roderick Munday (eds), *Comparative Legal Studies: Traditions and Transitions* (CUP, Cambridge 2003), 467-492, 489
[1050] As identified in the preceding chapters.
[1051] RK Yin, *Applications of Case Study Research* (Sage, Thousand Oaks 2002), xi
[1052] B Glaser and A Strauss, *The Discovery of Grounded Theory: Strategies of Qualitative Research* (Wiedenfeld and Nicholson, London 1967)
[1053] Case studies are not altogether absent in digital identity discourse, but none of these adopt a similar nuanced comparative approach. Vignettes were employed in Kai Rannenberg, D Royer, A Deuker (eds), *The Future of Identity in the Information Society: Challenges and Opportunities* (Springer, Berlin 2009); See also FIDIS, 'Identity Use Cases & Scenarios,' <http://www.fidis.net/resources/identity-use-cases-scenarios/>; U Gasser, JG Palfrey, 'Case Study: Digital Identity Interoperability and eInnovation,' Berkman Center Research Publication No. 2007-11, <http://cyber.law.harvard.edu/interop/pdfs/interop-digital-id.pdf>

communities. They[1054] will also enable and advance our understanding of the complexities at play in the legal regulation of digital identity. One must note however, that the analysis carried out here though deeper than that conducted in Chapter 5 is not strictly of the nature as would be conducted by a court. Rather, it has a socio-legal nature.

6.3. Case studies

The first case study deals with the privacy; the second with sharing; the third with reputation; the fourth with anonymity; the fifth with pseudonymity; the sixth with access to Internet resources and the seventh with control of personal data. Each of the case studies begins with a digital identity problem and examines it from the perspectives of UK and Indian law.

6.3.1. Privacy

John photographs Akbar embracing a woman in a street corner and publishes the photograph on Facebook. Akbar sees the photograph on Facebook and is extremely distressed that his privacy has been violated. Does Akbar have a right to privacy? What recourse to law, if any, does Akbar have?

This case study focuses on how the law regulates the privacy of online identity. It first examines Akbar's right to privacy under UK law followed by a similar examination under Indian law.

6.3.1.1.UK

Akbar has two remedies in respect of his right to privacy. The first, relates to a remedy under Article 8 of the ECHR as implemented by the HRA 1998 and the second, under the tort of misuse of private information. First, Akbar's right to privacy under Article 8 of the ECHR is analysed.

[1054] Each case study is inspired by different sources, singly or in combination: legal cases (reputation), factual reports (anonymity and access) empirical studies (privacy, sharing) and direct observation (control). The characters in the case studies are fictional.

Akbar has an established right to privacy under Article 8 of the ECHR, the right to respect of private and family life, and can invoke this in a court of law against John as the "values embodied in Articles 8 and 10 are as much applicable in disputes between individuals or between an individual."[1055] This is confirmed by a number of ECtHR and UK cases, some of which are outlined below.

In *PG and JH v the United Kingdom*, [1056] ECtHR outlined that there was a "zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life."[1057] While a person walking down a street may have limited privacy *stricto sensu*, "private life considerations may arise however once any systematic or permanent record comes into existence of such material from the public domain." This is evident in Akbar's case when John uploads the photograph of Akbar embracing the woman and creates a permanent record of the event.

In *Von Hannover v Germany,*[1058] relating to the violation of Article 8 of the ECHR by Germany through the circumvention of the applicant's right to private life and image, the ECtHR held that there is an obligation to protect private life and the use of one's image.[1059] In this case, like Akbar's, the issue was the publication of images taken in a public place during the course of carrying on activities of daily personal life. The ECtHR highlighted the "fundamental importance of protecting private life from the point of view of the development of every human being's personality," even such as "extends beyond the private family circle and also includes a social dimension."[1060] According to this, everyone, irrespective of whether they are known to the public, should be able to enjoy a "legitimate expectation" of the protection and respect for their private life. When this is not the case, there is a breach of Article 8. According to this reasoning, Akbar, even as a private individual has a right to

[1055] *Campbell v MGN* [2004] UKHL 22; *A v B plc* [2003] QB 195, 202, para 4 and Gavin Phillipson's 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act,' (2003) 66 MLR, 726-728
[1056] **n710**
[1057] ibid
[1058] (2005) 40 EHRR 1
[1059] Para 72
[1060] Para 69

privacy of his image in a public place and can successfully bring an action to enforce the enjoyment of that right.

This is also supported by case law in the UK. In *Campbell v MGN*,[1061] relating publication of articles and photographs of a fashion model visiting a Narcotics Anonymous meeting in a national newspaper, the House of Lords made some important observations in respect of the right to privacy.[1062]

Lord Nicholls recognised that "a proper degree of privacy is essential for the well-being and development of an individual"[1063] and that photographs of people "contain more information than textual description," are "more vivid" and "worth a thousand words." But photographs to be in breach of a privacy right had to be of "essentially private nature," "show something untoward" or "convey private information,"[1064] which in Akbar's case they clearly do.

Lord Hoffman in the same case reiterated that there was "no logical ground for saying that a person should have less protection against a private individual than he would have against the state for the publication of personal information for which there is no justification."[1065] Similarly, that the "widespread publication of a photograph of someone which reveals him to be in a situation of humiliation or severe embarrassment, even if taken in a public place, may be an infringement of the privacy of his personal information."[1066]

John's publication of the photograph of Akbar and the woman, according to this reasoning, is an infringement of Akbar's privacy. Though Akbar's photograph was taken in a public place, it contained information of essentially private nature of two individuals who (while they had been in a public place when the photograph had

[1061] [2004] UKHL 22
[1062] The House of Lords here reversed the Court of Appeal decision by a 3-2 majority.
[1063] Lord Nicholls, dissenting para 12
[1064] Lord Nicholls, dissenting para 31
[1065] Lord Hoffman, dissenting, para 50
[1066] Lord Hoffman, para 75

been taken) had not consented to the secondary use of this information, and who had no reason, at the time of their actions, to suspect that they were being photographed.

Akbar's claim to a right to privacy is further strengthened by the ruling of the Court of Appeal in *Murray v Big Pictures (UK) Ltd.*[1067] While recognising that the mere taking of a photograph of activity in a public place might be unobjectionable,[1068] the Court adjoined that "publicity of such activities is intrusive and can adversely affect the exercise of such social activities."[1069]

Thus, in proving that Akbar has a right to privacy under Article 8 of the ECHR, the first element of the tort of wrongful publication of private information, outlined by the Court of Appeal in *McKennitt v Ash*[1070] is engaged. The second element of the tort relates to the whether in the circumstances Akbar's interests must yield to John's right to freedom of expression conferred by Article 10 of the ECHR.

John's right to freedom of expression under Article 10 includes the freedom to hold opinions and to receive and impart information and ideas without interference by a public authority and regardless of frontiers. But this right is not a blanket right that trumps the right to privacy in all cases. The circumstances under which it may trump the right to privacy are limited as prescribed in Article 10(2), all of which do not apply in the instant case.[1071] For instance, there was no public interest in the publication of the photograph of Akbar embracing the woman. The publication of the photograph also did not fall within the sphere of political or public debate.[1072] Thus Article 10 is not engaged, and Akbar has a strong case against John for the wrongful publication of his private information.

In this manner it is evident that UK law affords definite and strong privacy protection to Akbar in respect of the publication of his online image.

[1067] [2008] EWCA Civ 446 (07 May 2008)
[1068] para 54
[1069] para 55
[1070] [2006] EWCA Civ 1714, per Buxton, LJ; Latham and Longmore LJJ in agreement.
[1071] See **n736**
[1072] *Von Hannover* **n1058**, paras 63, 64

6.3.1.2.India

What about Akbar's rights under Indian law? Does Akbar have a right to privacy as evidenced in the case of UK law? Does he have an effective remedy in the instant case at all? The answer, to the latter two questions, is no.

Section 66E of the ITA 2000 (as amended by ITAA 2008) might be said to specifically apply to Akbar's case. It prescribes punishment for violation of privacy online and reads:

> Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of a person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakhs rupees, or with both.

John captured (defined as videotaping, photographing, filming or recording by any means)[1073] transmitted (defined as electronically sending a visual image with the intent that it be viewed by other persons)[1074] and published (defined as reproducing in printed or electronic form and making it available to the public)[1075] the image of Akbar embracing a woman. So, the first part of the section has clear application.

However, next follow the problems. First, section 66E only applies in cases of violation of privacy through publication of images of the 'private area' of a person, which is restrictively defined by the Act as "the naked or undergarment clad genitals, pubic area, buttocks or female breast."[1076] Second, the circumstances violating privacy are confined in Section 66E (e) to two circumstances in which a person has a reasonable expectation of privacy: (i) that he or she can disrobe in privacy without fear that an image of their private area was being captured[1077] and (ii) that any part of a person's private area would not be visible to the public irrespective of where that person is.[1078]

[1073] S 66E (a)
[1074] S 66E (b)
[1075] S 66E (d)
[1076] S 66E (c). Recall here the cultural dimension of what is considered private in India.**Ch 3, 3.2.2.1.3**
[1077] S 66E (e) (i). This section is aimed at cases like home and fitting room privacy.
[1078] S 66E (e) (ii). This section is aimed at cases like underskirt filming.

Thus, Akbar has no right to privacy under Section 66E for the following reasons: first, the image is not an image of a private area of a person; and two, though there was no consent, it does not fall within the two circumstances the section explicitly provides for.[1079] Thus the protection afforded by Section 66E is limited in its scope and application. It offers no protection to the privacy of digital identity beyond a highly curtailed circumference.[1080]

What about Akbar's fundamental right to privacy under Article 21 of the Constitution? Akbar has a constitutional right to privacy against the State and private persons,[1081] but does this right apply in the instant case?

Under Article 21, the bar for proving a right to privacy exists is quite high, as will become evident in the following analysis.

One, it must be proved that there has been a calculated interference in the enjoyment of one's personal life or liberty. In *Kharak Singh,*[1082] relating to domiciliary surveillance, it was held that a right to privacy is available when there is a calculated interference with the enjoyment of a person's life or personal liberty. Mere personal sensitivity does not lend itself to a privacy right. According to the Court, a calculated interference would be one which involved not a single attempt but continuous and repetitive measures. In the instant case, there is no evidence of a "calculated interference" with Akbar's right to privacy.

Next, a person must not have voluntarily thrust himself into, invited or raised a controversy, such that led to or facilitated the violation of privacy. This is in line with

---

[1079] The section leaves little scope for expansive interpretation.

[1080] This sense of privacy stems from a low personal and social value attributed to privacy as substantiated in **Ch 3** (**3.2.2.1**) It is a reminder of how the law mirrors religious connotations of privacy. This section in particular accords with the following passage of the *Mahabharata*: *Nanagnibhikshte nari na vidvanpurushanapi, maithunam stanta guptmaharn cha samachmit* meaning: A naked woman ought not to be seen…Cited by the Supreme Court in *Phoolan Devi v Shekhar Kapoor* 57 (1995) DLT 154, § 33

[1081] As demonstrated in *Bodhisattwa,* **n718** *and Zee Telefilms,* **n719**

[1082] **n720.** The Supreme Court confirmed that the "the right of privacy is not a guaranteed right under our Constitution." Contrast this with the UK position where the right to privacy is generally accepted as a fundamental right.

Rajagopal[1083] where it was laid down that a person must not "voluntarily thrust himself into controversy or voluntarily invite or raise a controversy."[1084]

Akbar has a right to privacy of his own pursuits (in this case meeting and embracing the woman). John had no right to publish a photograph of Akbar without his consent. But in this case, John has a defence; that Akbar by embracing the woman in a public place had voluntarily thrust himself into and invited controversy by not keeping his actions private.[1085] Courts in India find no favour with privacy litigants who demonstrate this kind of behaviour.[1086] The legal interpretation of privacy in India is largely in terms of it being "a state of being private or in retirement; seclusion, secrecy or solitude."[1087] In this, the concept is still primitive in its development (as compared to the UK). Nor has it moved to become as pervasive and socially valuable concept as it has in the UK.[1088]

The right to privacy under Article 21 thus, though offering some privacy protection, does not translate into effective protection in cases like Akbar's. This is a very serious state of affairs which means that Akbar has no remedy in Indian law for the violation of his privacy.[1089]

At the end of this case study, it is evident that an individual's right to privacy is highly protected in the UK. Under this right an individual in the UK has an effective

---

[1083] **n722**
[1084] § 26
[1085] *Khushwant Singh v Maneka Gandhi* AIR 2002 Delhi 58; *Phoolan Devi* **n1080**
[1086] *The Managing Director v Mrs V Muthulakshmi* CRP (PD) 3299/2007 (Chennai High Court) §15 reiterating that "the right to privacy is available as long as the privacy is maintained by the parties. If the privacy comes out to public, the question of retaining the privacy does not arise." *Mr KJ Doraisamy v The Assistant General Manager* WP 17761/2006 (Chennai High Court) §15 (once a matter becomes matter of public record, right to privacy in it no longer subsists). *Ms X v Mr Z* 96 (2002) DLT 354; *Khushwant* **n1085** § 1
[1087] *MK Chandran v Commr of Police*, *Kochi* AIR 1998 Ker 347 § 11; *M/s Makkal T Thodarpu Kuzhuman Ltd v Mrs V Muthulakshmi* CRP (PD) 3299/2007 (Mad)
[1088] The HRA 1998 makes privacy a socially valuable concept. See Lord Bingham, 'The Way We Live Now: Human Rights in the New Millennium,' (1999) 1 Web JCLI, penultimate para; ICO, 'The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection' (March 2010) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_dividend.pdf>
[1089] Note, the woman might be able to protect her privacy by virtue of S 509 IPC (insult to modesty of a woman). This section is largely used in cases of sexual nature and acts have to have constituted "indecent behaviour" or been "offensive to morality." *State of Punjab v Major Singh* 1966 SCR (2) 286; *Anuradha Kshirsagar v State of Maharashtra* 1991 CriLJ 410.

remedy in law for the violation of privacy of his or her digital identity. Even in the context of a public place, individuals are afforded protection by privacy law in respect of their digital images.

However, the case is very different in India. The right to privacy is highly constrained and limited. It does not protect or afford significant, leave alone optimal levels of protection to individuals in India in respect of their digital images except in limited, specific and highly regimented confines. It has also not moved, as has in the UK, to include a privacy right in terms of actions in public places.

6.3.2. Sharing

Amita, a subscriber of a mobile phone service, lives in a large family comprising of her father, mother, siblings and their spouses, all of who persistently use her mobile phone for various purposes like making calls, accessing emails and the Internet and mobile banking. Her brother Vijay even lends the phone to his friend Ram. Amita discovers that Vijay and Ram have been using her phone to download material which is the subject of copyright. Is Amita liable?

This case study focuses on sharing of digital identities. Earlier, it was highlighted how socio-cultural trends in India, as compared to the UK, favour the sharing of digital identity technologies like computers and mobile phones, between a greater number of people and to a greater degree.[1090] Does the law recognise this and does it make allowances for these localised contexts of digital identity use? Does the law differentiate in the imposition of liability in respect of devices if they are less of more likely to be shared?

6.3.2.1.UK

The law in the UK, as currently evident sets the bar of legal liability for shared digital identity very high. This is particularly evident in the liability for copyright infringement. For example, a pub was fined £8,000 because material subject to

[1090] **Ch 3 (3.2.1.4)**

copyright was downloaded over its shared wi-fi hotspot.[1091] Amita might be liable under sections 23 (possessing or dealing with infringing copy) or 24 (providing means for making infringing copies) of the CDPA 1988.

In 2010, the Digital Economy Act 2010 (DEA 2010) was introduced inter alia to deal with online infringement of copyright and provide penalties for infringement of copyright and performers' rights. The Act inserts new provisions relating to online copyright infringement into the Communications Act 2003. Under section 124A, if a copyright owner finds that the subscriber to an Internet access service is infringing the owner's copyright through the service or has allowed another person to use the service then the owner may make a copyright infringement report[1092] to the ISP. The ISP must then notify the subscriber of the report if the initial obligations code[1093] requires the provider to do so. The ISP might also be obliged under Ofcom's directions to take technical measures (like service speed limitation, access prevention and control, suspension or other limitation of service) to prevent the infringement of copyright.[1094] The provisions of this Act go against the open and public sharing of access to Internet access.[1095] However, this is not a huge problem in the UK given that access to the Internet is generally available through personal devices over which individuals can exercise relatively good degrees of control.[1096]

[1091] D Meyer, 'Pub 'Fined £8k' for Wi-Fi Copyright Infringement,' *ZDNet UK* (27 November 2009) <http://news.zdnet.co.uk/communications/0,1000000085,39909136,00.htm>. A German Court has also held that owners of open Wi-Fi services are responsible for copyright violations by unauthorised third parties if they fail to secure and restrict access. See John Leyden, 'German Wi-Fi Networks Liable for 3rd Party Piracy,' *The Register* (13 May 2010) <http://www.theregister.co.uk/2010/05/13/open_wifi_fines_germany/>

[1092] A report that (a) states that there appears to have been an infringement of the owner's copyright; (b) includes a description of the apparent infringement; (c) includes evidence of the apparent infringement that shows the subscriber's IP address and the time at which the evidence was gathered; (d) is sent to the Internet service provider within the period of 1 month beginning with the day on which the evidence was gathered; and (e) complies with any other requirement of the initial obligations code.

[1093] For contents, see s 7, DEA 2010

[1094] S 9, DEA 2010

[1095] An argument echoed in David Meyer, 'Open Wi-Fi 'Outlawed' by Digital Economy Bill,' *ZDNet UK* (26 February 2010); Matt Brian, 'Is UK Public WIFI Doomed?' *The Next Web* (28 February 2010); SC, 'Claims Made that the Digital Economy Bill Will Cause the End of Public WiFi,' *SC Magazine* (23 March 2010)

[1096] See **Ch 3 (3.2.1.4)**

Under these provisions, Amita might find herself disconnected from the use of her mobile services and lose her digital identity, because she would be clearly liable as the subscriber of the phone for any shared use of her Internet connection (whether legitimate or illegitimate) under Section 124A (1) (b) of the Act.

6.3.2.2.India

Would Amita be liable under Indian law? First and foremost, much like the UK, Amita might be held liable, even though is she is not a primary infringer, under the Indian Copyright Act 1957, Section 63, if she "knowingly abets"[1097] the infringement conducted by Vijay and Ram. She could find herself liable to a sentence of imprisonment for a term of less than six months or a fine of less than fifty thousand rupees.

However, there is another very peculiar aspect to this issue. This relates to the nature of Amita's mobile phone as shared family asset. Amita, the primary digital identity subject, lives in a Hindu undivided family (HUF), a very important concept of Hindu law and an entity with rights and liabilities. A HUF refers to a family led by a *karta* (head of the family, in this case Amita's father) that is normally joint in food, worship and estate. The property of the HUF may comprise of ancestral property, joint acquisitions and/or self acquisitions as part of the common stock. So therefore the law regulating digital identity in India should be attuned to these uses which might necessitate the rethinking of strict liability terms for use of shared digital identities. But it is not. Amita should not be held responsible for the multiple uses of her digital identity, particularly as she has no control over them, but she might well be.

What if Amita's phone is used to publish or transmit obscene and sexually explicit material or child pornography? Again, she would find herself liable under Sections 67, 67A and 67B of the ITA 2000 (as amended by ITAA 2008), because she is the subscriber of the mobile phone. This implies that Amita has a legal responsibility to use her mobile as a personal and private device. But this is impossible, given that

[1097] Per *Cheria P Joseph v Prabhakarn* AIR 1967 Kar 234. Clear and cogent proof of knowledge is necessary to establish the commission of offence.

digital identity resources like computers and mobile phones are constantly used and experienced as shared assets in India; and will be impossible unless such conditions are recognised and promoted by society and law. But social norms go against the enclosing of digital assets and consequently digital identities.[1098] For example, Amita is expected to defer to her father and brother, and she is socially conditioned to behave that way.[1099]

But it is not just Amita who might be liable in the instant case. Amita's father as the karta or head of the family might also be held to account for any copyright infringement or criminal act committed in relation to Amita's mobile phone, as her phone functions as a common family asset. Though the burden of proof would be high in such a case, if *mens rea* can be proved in respect of the copyright infringement[1100] any or all of Amita's family could be held liable for the infringement.

For instance, as occurred in *Avnish Bajaj v State*,[1101] where the managing director of Bazee.com was criminally prosecuted under sections 292 (sale of obscene material) and 294 (punishment for obscene acts) of the IPC and section 67 of the ITA 2000 (electronic publication of obscene material), after his company's website listed a sexually explicit video clip depicting two school children, for sale. While the court discharged the petitioner's responsibility under sections 292 and 294 IPC,[1102] the Court found the petitioner responsible under section 67 of the ITA 2000.

In *Avnish,* the Court made reference to Section 85 of the ITA 2000 which holds that a person in charge of or responsible to a company for conduct of its business, may incur liability and punishment for any contravention committed during their tenure, unless it can be proved that the contravention occurred without their knowledge and despite due diligence to prevent it being exercised. The law thus imposes a deemed criminal responsibility under this section, and the burden of proof lies with the

[1098] **Ch 3 (3.1.2.4)**
[1099] See empirical evidence in **Ch 3, n317-324**
[1100] *Bhekha Ahir v Emperor* AIR 1947 Pat 236 (G)
[1101] Crl MC 3066/2006 (Del)
[1102] Holding that automatic criminal responsibility did not arise for directors of a company.

individual charged to prove the discharge of such liability.[1103] The Court here relied on the Supreme Court's authorities of *Sheo Ratan Agarwal v State of MP,*[1104] *UP Pollution Control Board v Messers Modi Distillery*[1105] and *Anil Hada v Indian Acrylic Ltd.*[1106]

What is significant here is that while the law imposes a great burden in terms of liability on digital identity subjects like Amita in India, it fails to take into account that digital identity devices like mobiles and computers function as shared devices, making digital identity social and multiple in relation to the number of identity subjects with access to it. The law makes no allowance for the vast shared context of digital identity in India which is a result of its peculiar digital developmental and social conditions. It also fails to recognise socio-cultural factors that put digital identity subjects in India on unequal footing with one another (e.g. Amita's deference to her family as a female and junior member). Here is evident a mismatch in the expectations and application of the law and the local context of digital identity, in India.

6.3.3. Reputation

Brijesh creates a false profile for Jai on Orkut,[1107] a social networking site. While a few of the entries are true (like name, place of residence, data of birth), the substantial part are false e.g. sexual orientation (Jai is a heterosexual but according to the profile he is homosexual), political and religious views (Jai is alleged to support a banned extremist organisation). Jai's personal and professional life suffers. His fiancée calls off their engagement and he loses his job.

This case study is based on two legal cases: *Applause*[1108] and *Katti*.[1109]

[1103] Para 20.2
[1104] (1984) 4 SCC 352
[1105] (1987) 3 SCC 684
[1106] (2000) 1 SCC 1
[1107] <www.orkut.com>
[1108] **n980**
[1109] **n688**

In *Applause*, the primary issue was whether Grant Raphael (an ex-friend of Firsht) was liable for uploading a false profile and creating a defamatory group in relation to Mathew Firsht on Facebook. It was alleged that the material uploaded was defamatory of Mathew Firsht and Applause Store and had been created using a computer with Grant Raphael's IP address. The false profile comprised of information about Firsht's sexual orientation, relationship status, date of birth, political and religious views (some of which were claimed to be inaccurate).

The Court in dealing with the defamation claim awarded damages for libel to Firsht amounting to £15,000 and to Applause Store of £5,000. In relation to the tort of misuse of private information, the Court in acceding that Firsht as a private person had been caused 'great shock and upset' by the misuse of his personal information, awarded Firsht a sum of £2000. In making this award, the judgments in *McKennitt v Ash*,[1110] *Campbell v MGN Ltd*[1111] and *Campbell v MGN Ltd*[1112] were referred to.

In *Katti,* obscene, defamatory and annoying messages were posted about a woman in a Yahoo! Message group. The perpetrator, a spurned ex-family friend of the woman, opened a sham email account in the woman's name which led to her being harassed with phone calls from people who thought she was soliciting. The perpetrator was charged under section 469 (forgery for the purpose of harming reputation) and 509 (act to insult the modesty of women) of the IPC and section 67 of ITA 2000 (electronic publication of obscene material), convicted and sentenced. He was ordered to undergo rigorous imprisonment for two years and a fine of Rupees 500 (for offence under section 469 IPC), one year simple imprisonment and fine of Rupees 500 (for offence under section 509 IPC) and two years rigorous imprisonment and fine of Rupees 4,000 (for the offence under section 67, ITA 2000), all of which were to run concurrently.

Applause and *Katti* both have very similar facts: conflict arising out of personal relationships gone wrong. In both cases, reputation was harmed. The only difference

[1110] [2006] EMLR 178
[1111] [2002] EWHC 499 (QB)
[1112] [2004] 2 AC 457

is that *Firsht* was resolved in the private law framework (tort law) and *Katti* in the public law framework (criminal law). Does this suggest that there is a preference for digital identity disputes to be settled within the private law framework in England while in India, digital identity disputes of such nature are largely a public law matter? If so, what does this mean for the regulation of digital identity?

6.3.3.1.UK

The offence of common law defamatory libel in England and Wales and Northern Ireland was abolished by the Coroners and Justice Act 2009.[1113] Section 73 of the Act provides that the offences of sedition and seditious libel, defamatory libel and obscene libel have been abolished. Therefore, Brijesh cannot be criminally prosecuted for an offence of defamatory libel under the law of England and Wales and Northern Ireland.

But this does not mean that Jai has no remedy in respect of the harm caused to him by Brijesh. As evidenced in Chapter 5, Jai has civil law remedies (like damages and injunctions) he can avail of. This is also demonstrated by *Applause* and the case of the law student who was awarded damages of £10,000 by the London High Court when his private life and public reputation suffered as a result of an ex-friend making defamatory claims on Facebook about him being a paedophile with homosexual tendencies.[1114]

6.3.3.2.India

What would be Jai's position in India? How would this dispute be resolved? Would Brijesh be accountable for his actions?

The principal manner the instant case would be resolved in India, like *Katti,* is through the criminal law framework. Jai's remedy would lie in Section 469 of the IPC dealing with forgery to harm reputation. It states:

[1113] E.i.f 12 January 2010

[1114] Telegraph.co.uk, 'Law Student Wins £10,000 After Being Branded a Paedophile on Facebook,' (28 July 2010) <http://www.telegraph.co.uk/technology/facebook/7912731/Law-student-wins-10000-after-being-branded-a-paedophile-on-Facebook.html>

> Whoever commits forgery[1115][intending that the document or Electronic Record forged][1116] shall harm the reputation of any party, or knowing that it is likely to used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

Brijesh has committed forgery by creating an Orkut profile,[1117] for Jai with false information in it. This has resulted in repercussions upon Jai's personal and professional reputation and life. Brijesh would also attract the attention of Section 499 of the IPC dealing with defamation as he has, through the Orkut profile, made and published imputations about Jai either intending to cause Jai harm and knowing or having reason to believe that it would cause harm to Jai's reputation. In such a case, Brijesh could find himself facing simple imprisonment extending to up to two years, a fine or both.

What about civil remedies? Does Jai have any civil remedies in respect of Brijesh's actions? Indeed, he does. In India, a civil suit for defamation under tort law is also maintainable either in combination with criminal proceedings, or separately, or sequentially.

However, civil suits under the tort for defamation, which can only be filed before the High Court of a State, are sparse. Where evident, they run sequentially post criminal proceedings for enforcement of damages. To date, there is evidence of only three cases filed before High Courts in relation to online defamation (*SMC Pneumatics,*[1118] *Gremach*[1119] and *Socieadade*,[1120]) all of which related to the protection of commercial reputation.[1121] There is no evidence of civil defamation cases being filed by individuals to protect their online reputation.[1122]

[1115] Defined in S 463, IPC.
[1116] Substituted by Act 21 of 2000, s 91 and Sch. I, for 'intending that the document forged.'
[1117] An Orkut profile is an electronic record as defined by s 2 (t), ITA 2000: data, record or data generated, image or sound stored, received or sent in and electronic form or microfilm or computer generated micro fiche.
[1118] **n982**
[1119] **n983**
[1120] **n984**
[1121] **Ch 5 (5.2.6.1.2)**
[1122] As at 01.12.10

There are a number of reasons for this. The foremost relates to the lack of codification of the tort law of defamation and its case by case development, with wide scale borrowing from the English legal system. Though there has been some legislation in the tort field, the lack of assertion of individuals over their legal rights in India is attributable to the difficulty of proving claims, high legal expenses and court delays in obtaining justice.[1123] Compared to this, the criminal defamation regime is well established in form, principle and practice, and caters well to cases of digital defamation.[1124]

Delving deep into the matter, one finds the answer to why criminal remedies are the preferred digital identity problem solving solution in India. As far back as 1930, Walsh stated that "the Indian much prefers, if he can seek assistance, the criminal court for the redress of his civil wrongs."[1125] This preference has stayed strong and the criminal law system supports this with the help of an elaborate and easily accessible framework for the redressal of private complaints.[1126]

Civil remedies like torts are considered to be remedies of the lower order in India. Galanter succinctly summarises the reasons torts are lacking as a remedy: ad valorum court fees, continuing lawyer fees, successive delays, interlocutory appeals, low or meagre awards of damages (to avoid windfall gains)[1127] and pursuant judgment execution problems.[1128] These remedies are generally inaccessible and necessitate

---

[1123] B Veeraragavan, 'Torts In India Whether Unnecessary Or Simply Overlooked,' LegalService India (6 December 2007)

[1124] This is also evident in how S 66A, ITA 2000 (as amended by ITAA 2008) might be brought to apply to cases of online defamation where it can be proved that a person has sent false information through a computer resource or communication device to cause annoyance, inconvenience, deception, hatred, ill will, etc that person could be punished with imprisonment for a term extending to three years and a fine.

[1125] C Walsh, *Crime in India,* (Ernest Benn, London 1930), 26

[1126] Upendra Baxi and Thomas Paul, *Mass Disasters and Multinational Liability: The Bhopal case*, (Indian Law Institute, New Delhi 1986), 179; Marc Galanter, 'Legal Torpor: Why So Little Has Happened in India After the Bhopal Tragedy,' (1985) 20 Texas Intl LJ, 273-294, 275

[1127] As confirmed by the Delhi High Court in *Ram Jethmalani v Subramaniam Swamy* AIR 2006 Delhi 300 §104, stating that "Punitive damages in defamation are not awarded in India. Damages awarded are recompense to the loss of honour and reputation. Inherently, quantification is a problem, as honour and reputation are inherently incapable of being valued in terms of money." See the low awards made in *Noor Mohammed v Mohammed Jiajdin* 1991 (0) MPLJ 530 (Rs 3000, approx. £ 40); *GS Walavalkar v PS Rege* AIR Bom 224 (Rs 4000, approx. £55)

[1128] Marc Galanter, 'India's Tort Deficit: Sketch for a Historical Portrait,' in DM Engel and M McCann (eds), *Fault Lines* (SUP, Stanford 2009), 47- 65, 54

more conscious and active involvement of the litigant. They are also slow and largely ineffective in providing relief.[1129] The Indian legal system actively discourages individual claimants from using torts as a remedy to enforce individual interests.[1130] This has led to huge reliance on and preference for criminal remedies.

Thus, this case study shows how the nature digital identity regulation differs between the UK and India in respect of the protection of individual reputation. In the UK, protection of reputation is a private law matter, a matter of individuals asserting their rights; in India, au contraire, it is a public law matter, the State protecting the interests of the individual against other individuals.

6.3.4. Anonymity

X is HIV positive (a fact secret from her family and friends). She goes to a cybercafé to find out information about AIDS. She finds out has to register her identity to use the services. She is uncomfortable with the idea, but with no other means of Internet access, complies and is able to surf the Internet to find the information and support required. A week later she is thrown out of her family home and is shunned by her friends and acquaintances in her locality. The cyber café operator had matched her registered identity with her web surfing habits and felt he had the moral duty to warn people about her condition. Does X have a right to anonymity and a remedy for its violation?

This case study is centred upon the issue of anonymity which, as evident in Chapter 2, is one of the most important features of digital identity. This case study examines the law's application in the creation and support of the conditions of identification and anonymity in the UK and India.

[1129] National Commission to Review the Working of the Constitution, 'Liability of the State in Tort,' Consultation Paper (New Delhi, 2001) para 6.1; R Ranchhoddas, DK Thakore and GP Singh, *Ratanlal & Dhirajlal's the Law of Torts* (Wadhwa & Co, 2008); KB Agrawal and V Singh, *Private International Law in India* (KLI, 2010), 135; Amanda Perry-Kessaris, 'Access to Environmental Justice in India's Garden City (Bangalore),' in Andrew Harding (ed), *Access to Environmental Justice: A Comparative Study* (Martinus Nijhoff, Leiden 2007), 59-88, 64

[1130] See comments of Bombay High Court in *Manisha Koirala v Shashilal Nair* 2003 (2) BomCR 136

6.3.4.1.UK

In Europe and the UK, digital anonymity is perceived as a tool to help the digital identity subject protect himself, his personal life and privacy against interference from others.[1131] It is a vital ingredient of the freedom of expression.[1132] The recommendations of the Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data support this contention in relation to Europe.

Recommendation 3/97 on Anonymity on the Internet[1133] calls for maintenance of choice to remain anonymous while recognising that the need for anonymity in respect of online transactions underpins privacy and freedom of expression. In Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications,[1134] the Working Party recognises the need for anonymity in respect of use of telecommunications services.

Further, in Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6[1135] it recommended that **"**network and access providers should offer to any user the option to use the network or to access the services anonymously or using a pseudonym." In Opinion 1/2003 on the Storage of Traffic Data for Billing Purposes[1136] adopted on 29 January 2003, the Working Party supports a regime of anonymised traffic data.

[1131] D Wright and ors, (eds), *Safeguards in a World of Ambient Intelligence* (Springer, Dordrecht 2010), 212
[1132] J Lipschultz, *Free Expression in the Age of the Internet: Social and Legal Boundaries* (West View Press, Oxford 2000)
[1133] Adopted by the Working Party on 3 December 1997 <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp6_en.pdf>
[1134] Adopted on 3 May 1999, <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp18en.pdf>
[1135] Adopted on 30 May 2002, <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_en.pdf>
[1136] 12054/02/EN WP 69 <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp69_en.pdf>

Cybercafés in the UK generally operate under a principle of minimal identification of users of their services[1137] and mandate low levels of identification in relation to the use of such digital services.

In the instant case study, X's right to anonymity is guaranteed and protected in the UK. This is because cybercafés are required to comply with the DPA 1998, as they are both data controllers[1138] and data processors[1139] dealing with personal data under the Act and thus are required to comply with the obligations imposed upon them by the Act. X's data that is controlled and processed by the cybercafé operator is a combination of personal and sensitive personal data.[1140] In further disclosing X's personal and sensitive personal data beyond the remit it had been lawfully obtained for, the cybercafé operator failed to meet the obligations imposed by the Act and is clearly in breach.

The cybercafé (and the operator) had an obligation to comply with the data protection principles set out in Schedule 1 of the DPA 1998. X's personal data should have been fairly and lawfully processed.[1141] Here, this is clearly not the case. X's personal and sensitive personal data might have been obtained for a specified and lawful purpose, but it was further processed in a manner incompatible with the purpose for which it was obtained.[1142]

The first data protection principle (Para 1 of Schedule 1 of DPA 1998) expressly prohibits the processing of sensitive personal data unless one of the conditions in

[1137] Cybercafés would be required to comply with the obligations imposed by the Data Retention (EC Directive) Regulations 2009
[1138] The cybercafé is a data controller because it determines the purposes and manner in which the personal data of the people he relates to is processed. DPA 1998, s 1 (1)
[1139] Processing of personal data refers to, "obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including the organisation, adaptation or alteration of the information or data, retrieval, consultation or use of the information or data, disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data. DPA 1998, s 1(1)
[1140] Sensitive personal data is defined in S 2, DPA 1998 as personal data that consists of information about a data subject's racial or ethnic origins, political opinions, religious or other similar beliefs, trade union membership, physical or mental health or condition, sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
[1141] First Data Protection principle
[1142] Second Data Protection principle

Schedule 3 of the Act is fulfilled. Schedule 3 of the DPA 1998[1143] prescribes the specific conditions under which sensitive personal data may be processed.[1144] One of these conditions is explicit consent of the data subject,[1145] which in this case is clearly missing.

Another condition applicable to the processing of sensitive personal data is that the processing is carried out (with appropriate safeguards for the rights and freedoms of data subjects) in the course of its legitimate activities by a body or association not established or conducted for profit, and exists for political, philosophical, religious or trade-union purposes and relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes.[1146] In these conditions, the UK data protection regime robustly protects digital identity manifesting as sensitive personal data.

The cybercafé also failed to meet the obligation under the Sixth data protection principle (processing of personal data in accordance with the rights of data subjects). This is particularly evident in respect of Section 10 of the DPA 1998 which provides data subjects with the right to prevent processing of data such as is likely to cause damage or distress.

The cyber café operator can be held liable of an offence under section 55 of the DPA 1998[1147] which provides that a person must not knowingly or recklessly, without the consent of the data controller either (a) obtain or disclose personal data or the information contained in personal data, or (b) procure the disclosure to another person of the information contained in personal data.[1148] Offences under this section

[1143] Schedule 3 prescribes the Conditions relevant to the processing of sensitive personal data.
[1144] In addition to the conditions in Schedule 3, there are regulations setting out conditions for the processing of sensitive personal data -The Data Protection (Processing of Sensitive Personal Data) Order 2000.
[1145] Schedule 3 (1), DPA 1998
[1146] Schedule 3 (4), DPA 1998
[1147] Up to date details of prosecutions at ICO website <www.ico.gov.uk>
[1148] S 55 (1)

are punishable with a fine of up to five thousand pounds in a Magistrates Court; unlimited in the Crown Court.[1149]

The cybercafé operator cannot escape liability under the exceptions because he cannot prove that disclosure he made of X's personal and sensitive personal data to the people in the locality was necessary for crime prevention or detection,[1150] was required or authorised by law,[1151] that a legal right to disclose the information existed [1152] or that the disclosure was justified in the public interest.[1153]

The cybercafé (and the cybercafé operator) violated the rights of X (as a data subject) in keeping her personal and sensitive personal data anonymous. X also has a remedy under section 13 of DPA 1998 for any damage and distress she has suffered as a result of the violation. Data subjects in the UK are thus supported by law in keeping their personal and sensitive personal data private and anonymous.[1154]

6.3.4.2.India

Unlike the UK, it will now be argued that X has no parallel right to anonymity under Indian law.

Cybercafés are the primary means of Internet access in India.[1155] Under the ITA 2000, a cybercafé is defined as "any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the

[1149] A consultation was held to provide a custodial deterrent to data protection offences. See Department for Constitutional Affairs, 'Increasing Penalties for Deliberate and Wilful Misuse of Personal Data,' Consultation Paper, CP 9/06 (July 2006) <http://www.dfpni.gov.uk/consultation_misue_of_personal_data.pdf>
[1150] S 55 (2) (a) (i)
[1151] S 55 (2) (a) (ii)
[1152] S 55 (2) (b)
[1153] S 55 (2) (d)
[1154] X might also have a breach of confidence remedy against the cybercafé operator. See **Ch 5 (5.2.5.5.1)**
[1155] See IMRB and IAMAI, 'Internet in India: 2006,' Summary Report (6 December 2006) 16 <http://www.iamai.in/Upload/Research/book.pdf>

public."[1156] Cyber cafés are also intermediaries[1157] under the ambit of the Act and have to comply with the rules laid down in respect of them.

Under section 90 of the ITA 2000 (as amended ITAA 2008), state governments have the power to make rules to carry out the provisions of the Act. Under this section or under various state Police Acts, many states have made regulations to govern the use of cybercafés.

For example, in Maharashtra has special Rules under the Police Act[1158] which hold that every cyber café user is required to prove their identity prior to use of services by producing a photo-identity card e.g. passport, college ID, PAN Card, election card, Motor Driving Licence, office identity card, etc. The cyber café user is required to enter the user's details in a log (retained for a year).

Similar is the case in Delhi where according to an Order issued by the Delhi police under Section 144 of the Code of Criminal Procedure 1973,[1159] the identity of a cyber café user must be established prior to use of services. The user's personal information is logged in a register that is maintained with logs of all activity conducted online for a prescribed minimum period.

The state of Karnataka also has the Information Technology (Karnataka) Rules 2004[1160] which correspondingly provide that no user will be permitted to use a cybercafé computer, computer System and/or computer network without their identity being established.[1161] The cybercafé owner/operator must also obtain and

---

[1156] Section 2 (na)
[1157] Defined in s 2 (w) as "any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers; network service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafés."
[1158] See 'Special Rules for Cyber Café, Computer or Virtual Reality Game,'s 246 in particular. See <http://www.mumbaipolice.org/downloads/Notification%20of%20Cyber%20Cafe.pdf>
[1159] No.2, 1974; Read with Govt. of India, Ministry of Home Affairs, New Delhi's Notification No. U-11036/1/2008- UTL (26 November 2008)
[1160] Made under the powers conferred by the ITA 2000, s 90; <http://www.ccaoi.in/UI/docs/Karnataka%20Cyber%20Cafe%20Regulations.doc>
[1161] Rule 3(2)

maintain details of the user (like name, age, sex, present residential address, and usage times).[1162]

Similar rules and regulations exist in other states like Gujarat,[1163] Rajasthan,[1164] Sikkim[1165] and Tamil Nadu.[1166] A strong regime of establishing identity of identity subjects prior to Internet use thus exists. The overall legislative policy in India does not favour anonymous access to the Internet. There is no automatic right to anonymity for cybercafé users in India; rather a trend of identification of users is the norm.

What about X's right to anonymity in relation to the cybercafé operator's behaviour? There is no express data protection legislation that enables digital identity subjects in India to protect their identity through promoting conditions of anonymity, as in the UK.

Neither does the law in the ITA 2000 (as amended by ITAA 2008) support anonymity nor does it effectively protect X's right to anonymity in respect of her medical information or data. The Act fails to cater to situations as in the instant case study, and ignores largely the personal interests that individual digital identity subjects might have in safeguarding their identities, through the reduced or minimal use of identification.

There is a provision for compensation in respect of failure to protect data in the ITA 2000 (as amended by ITAA 2008) - section 43A. This section provides, in principle, that an entity possessing, dealing or handling sensitive personal data or

---

[1162] Rule 4(1)
[1163] The Gujarat Information Technology Rules 2004, <http://www.ccaoi.in/UI/docs/Cyber%20Law%20-%20Guj.pdf> (establishment of identity and storage of Internet logs and records)
[1164] Rajasthan Cyber Café Rules 2007, <http://www.rajasthan.gov.in/rajgovresources/newitems/Raj_Cyber_Cafe_Rules.pdf>
[1165] Sikkim Information Technology Rules 2009 (unavailable online)
[1166] The Browsing Centre (Tamil Nadu) Rules/Conditions, <http://www.tnpolice.gov.in/forms/BROWSINGCENTREREGULATIONRULESANDAPPLICATION.pdf> (establishment of identity and retention of activity logs and Internet records)

information,[1167] found to be negligent in maintaining reasonable security practices and procedures[1168] and causes wrongful loss or wrongful gain to any person, shall be liable to pay damages not exceeding five crore rupees to the affected person. Yet, though this section applies in theory to the instant case study, it would be hard to apply in practice as 'sensitive personal data' under the scope of this Section has not yet been prescribed by the Central Government.[1169]

Thus, the ITA 2000 (as amended by ITAA 2008) makes it extremely unlikely to express or protect anonymity through protection of personal data which in the digitally advanced West, and the UK, is considered an important facet of digital identity.

6.3.5. Pseudonymity

Mohammed Adeel, a devout Muslim, is registered on Twitter as Gansham Das. His nasty experience of being flamed in a chat room based on his religious identity led him to choose a Hindu name to represent himself thus. Adeel in his identity as Gansham Das make some inappropriate comments about religion. An irate acquaintance aware of Adeel's dual identities reports Adeel to the police for using a pseudonym. Has Adeel committed a crime?

Pseudonyms are another vital expression of digital identity. This case study explores from the criminal law perspective how the law works to promote or curb the use of false pseudonyms in the UK and India.

[1167] Such personal information as prescribed by the Central Government in consultation with such professional bodies or associations as it deems fit. S 43A (iii), ITA 2000 (as amended ITAA 2008)
[1168] Practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.
[1169] As at 01.12.10

6.3.5.1.UK

What is Adeel's position under UK law? Adeel's actions of adopting a pseudonym are not per se illegal under UK law. This is evident in the examination of the relevant law applicable to this case, primarily the criminal law regime.

First, let's look at the UK Fraud Act 2006 which provides for criminal liability for fraud and dishonestly obtaining services. This would include any form of digital identity fraud. Section 1 (1) of the Act provides that a person is guilty of fraud if he commits: fraud by false representation, fraud by failing to disclose information or fraud by abuse of position. All conditions being satisfied, fraud by false representation covers activities like phishing, pharming and credit card fraud.[1170] Section 2 clarifies that fraud by false representation occurs when a person dishonestly makes a false representation, and intends, by making the representation either to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss.

In this case, though Adeel might have made a false representation, there is no evidence of dishonesty. Per the Guidance Notes to the Act, dishonesty is to be measured according to the two stage test set out in *R* v *Ghosh.*[1171] The first test is whether Adeel behaved dishonestly by the ordinary standards of reasonable and honest people. It is unlikely that Adeel would be found guilty of dishonesty if reasonable and ordinary people opined (which they do since there are numerous examples of people adopting pseudonyms in digital transactions)[1172] that Adeel's behaviour was normal or a vital element of the right to freedom of expression. The next test to be applied is whether Adeel was aware that his conduct was dishonest and would be considered dishonest by reasonable and honest people.[1173]

[1170] Bainbridge (2007) **n677,** 277
[1171] [1982] QB1053
[1172] **Ch 2 (2.5.10)**; A Surveillance Society (2007-08) **n630**, 45; Steve Wheeler and Helen Keegan, 'Imagined Worlds: Emerging Cultures,' in Steve Wheeler (ed), *Connected Minds, Emerging Cultures: Cybercultures in Online Learning* (Information Age Publishing, USA 2009), 261-276, 269
[1173] Fraud Act 2006, Explanatory Notes.

Adeel must have also made the false representation with the intent of making some gain or causing loss or risk of loss to another.[1174] It is immaterial if the gain or loss has occurred. In the instant case, Adeel had no such intent. Therefore, Adeel cannot be prosecuted for the use of a pseudonym under the under the Fraud Act 2006.

It can be concluded that in general, UK law, at least in relation to the law of fraud, does not proscribe the use of digital pseudonyms, though there may be particular circumstances when the use of a pseudonym might be illegal.

6.3.5.2.India

What is Adeel's position in India?

Adeel's actions may fall within the ambit of section 66A (b) of the ITA 2000 (as amended by ITAA 2008). This section prescribes that any person, who persistently by means of a computer resource or communications device sends false information to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will shall be punishable with imprisonment for a term which may extend to three years and a fine.[1175] Adeel's pseudonym 'Gansham Das' is false digital information[1176] that has caused annoyance to Adeel's acquaintance. A court might also find it provocative of enmity, ill will or hatred, and to protect religious sensitivities and maintain religious harmony might hold him responsible for his actions.[1177]

Adeel's actions may alternately attract Section 66A (c) of the Act. This section applies when a person deceptively or misleadingly sends an email or email message that causes annoyance, inconvenience to the addressee or recipient. This act is

[1174] S 2 (1) (b) requires that the person must make the representation with the intention of making a gain or causing loss or risk of loss to another.
[1175] Inserted by ITAA 2008.
[1176] The IPC uses false in the sense of unrelated to the real.
[1177] Adeel might be in contravention of the constitutional ideal of upholding fraternity amongst citizens and the fundamental duty imposed on every Indian citizen to promote harmony and the spirit of common brotherhood amongst all the people of India transcending religious, linguistic and regional or sectional diversities. Part IV A, Article 51A (b), Constitution of India. *SR Bommai v Union of India* CA 3645 of 1989 (SC). Courts have upheld the need protect religious sentiments in *Gopal* (1969) 72 Bom LR 871(SB); *Ramjilal Modi v State of UP* AIR 1957 SC 620. Particularly telling is the judgment of Supreme Court in the *D Ajith* case (unreported). See Dhananjay Mahapatra, 'Bloggers Can be Nailed for Views,' *Times of India* (24 February 2009) <http://timesofindia.indiatimes.com/India/Bloggers-can-be-nailed-for-slur/articleshow/4178823.cms>

punishable with imprisonment for a term which may extend to three years and with fine.[1178]

There is also Section 66D in the ITA 2000 (as amended by ITAA 2008) which provides punishment for cheating by personation. It states,

> Whoever, by means of any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

This provision is similar to the offence of cheating by personation under section 416 of the IPC (which provides that a person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is).[1179]

Thus, in India Adeel's use of a pseudonymous digital identity is more problematic and conducive to attracting penal sanctions. The law in India thus takes a dim view of the use of pseudonyms.[1180]

The analysis of this case study shows an apparent distinction in how digital pseudonyms are legally dealt with in two different countries. In the UK, there is no general outright legal proscription against the use of digital pseudonyms unrelated to the individual (this is somewhat natural given that the use of digital pseudonyms as means of concealing identity developed in the West and the widespread adoption of false pseudonyms).[1181] On the other hand, though there is no general outright proscription against pseudonyms, the law as it currently stands in India clearly does not advocate the use of pseudonyms of the nature adopted by Mohammed Adeel.

[1178] Inserted by ITAA 2008.
[1179] The offence is committed whether the individual personated is a real or imaginary person.
[1180] In sharp contrast to the how the law in Europe actually advocates the use of pseudonymous identity. See **Ch 5 (5.2.4.1)**
[1181] As shown in **Ch 4**

6.3.6. Access to Internet resources

Mahesh has a Google account, which for him represents his principal digital identity. He uses his Google account for various purposes like email, chat, blogging, photo sharing, social networking, and document storage. One day Mahesh finds that he can no longer access his Google id. It has been blocked by the government.

This case study is themed on blocking of digital identities by the State. It analyses the position of individuals like Mahesh who find access to their digital identities curtailed by measures adopted by the State. Does Mahesh's have better or more guaranteed conditions of access to his digital identity in the UK as compared to what is possible under Indian law?

6.3.6.1.UK

There are very limited legal provisions that apply in respect of the blocking of Internet access in the UK. Blocking is only permitted in exceptional circumstances as will become evident in the analysis below.

Explicit provisions permitting blocking in respect of copyright violations are provided in the DEA 2010. Section 17 provides the Secretary of the State the power to make provision about injunctions preventing access to locations on the Internet. It states,

> The Secretary of State may by regulations[1182] make provision about the granting by a court of a blocking injunction in respect of a location on the Internet which the court is satisfied has been, is being or is likely to be used for or in connection with an activity that infringes copyright.[1183]

A blocking injunction, per the Act, refers to "an injunction that requires a service provider to prevent its service being used to gain access to the location."[1184] However, the power under this section is limited by conditions. For instance, regulations cannot be made under this section unless the Secretary of the State is

[1182] These Regulations must be made by statutory instrument. S 17(10).
[1183] S 17(1)
[1184] S 17(2)

satisfied of the following: one, that the use of the Internet for activities that infringe copyright is having a serious adverse effect on businesses or consumers; two that making the regulations is a proportionate way to address that effect; and three, that making the regulations would not prejudice national security or the prevention or detection of crime.[1185]

Any blocking Regulations must prescribe that a Court grant a blocking injunction when it is satisfied that the location seeking to be blocked is either a location from which a substantial amount of material has been, is being or is likely to be obtained in infringement of copyright, is a location at which a substantial amount of material has been, is being or is likely to be made available in infringement of copyright, or a location which has been, is being or is likely to be used to facilitate access to an infringing location.[1186] In addition, S 17(5) of the Act provides that the regulations must provide that, in determining whether to grant an injunction,[1187] the court must take account of the following factors:

> (a) any evidence presented of steps taken by the service provider, or by an operator of the location, to prevent infringement of copyright in the qualifying material,
> (b) any evidence presented of steps taken by the copyright owner, or by a licensee of copyright in the qualifying material, to facilitate lawful access to the qualifying material,
> (c) any representations made by a Minister of the Crown,
> (d) whether the injunction would be likely to have a disproportionate effect on any person's legitimate interests, and
> (e) the importance of freedom of expression.

More vitally, it is prescribed that the Regulations must provide that a court may not grant an injunction unless notice of the application for the injunction has been given, in such form and by such means as is specified in the regulations, to the service provider[1188] and the operators[1189] of the location. Mahesh as an affected subscriber may make an appeal under Section 124K of the Communications Act 2003.[1190]

[1185] S 17(3)
[1186] S 17(4)
[1187] Interdict, in the case of Scotland. S 17(13), DEA 2010
[1188] "service provider" has the same meaning as in s 97A of the CDPA 1988. See s 12 of Act.
[1189] In relation to a location on the Internet, entities who have editorial control over material available at the location (s 12).
[1190] Inserted by DEA 2010.

Thus, there is a legal remit on the blocking of Internet access specifically in relation to copyright violations.

Blocking of Internet services in the UK beyond this operates under a regime of self-regulation. The Internet Watch Foundation (IWF),[1191] an independent body, was set up by the UK Internet industry in 1996 to provide an UK Internet Hotline for the reporting and taking down of potentially illegal online content.[1192] Though it works with the UK government, the IWF is not a legally empowered body.[1193]

The IWF facilitates[1194] the taking of blocking actions as a "short term disruption tactic" by the Internet industry (comprising of Internet service providers, mobile operators, search providers, filtering companies) in respect of four types of Internet content: child sexual abuse content hosted anywhere in the world,[1195] criminally obscene adult content hosted in the UK,[1196] incitement to racial hatred content hosted in the UK[1197] and non-photographic child sexual abuse images hosted in the UK, [1198] according to UK law.[1199]

Blocking, as evident above, is a non-governmental, limited and industry led voluntary measure.[1200] The UK government, according to itself, is "clear that the use of blocking to prevent access to such images is something that Internet service

[1191] IWF <http://www.iwf.org.uk/>
[1192] For full list of IWF members, see <http://www.iwf.org.uk/funding/page.64.htm>
[1193] It is an incorporated charity, limited by guarantee.
[1194] Per the IWF, its blocking role is "restricted to the compilation and provision of a list: the blocking solution is entirely a matter for the company deploying the list. Our list is designed and provided for blocking specific URLs only. Any decision to convert or adapt the list to block whole domains may lead to the overblocking of legitimate content and is not supported by the IWF." <http://www.iwf.org.uk/public/page.148.htm>
[1195] Protection of Children Act 1978, Civic Government (Scotland) Act 1982, Sexual Offences Act 2003: Key Changes (England and Wales), Memorandum of Understanding: Section 46 Sexual Offences Act 2003, Police and Justice Act 2006
[1196] Obscene Publications Act 1959 and 1964, Criminal Justice and Immigration Act 2008, S 63
[1197] Public Order Act 1986 and the Race Relations Act 1976.
[1198] Coroners and Justice Act 2009
[1199] Also Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects Of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce)
[1200] UK policy veers decidedly towards being a "light touch" in access blocking. See DW Vick, 'Regulatory Convergence?' (2006) 26 (1) Legal Studies, 26-64

providers should do, and the Government has been very pleased with the response from the Internet industry."[1201]

If Mahesh's block was the result of an assessment made by the IWF on illegal content and he was prevented from accessing legal content he could appeal to the IWF against the denial of his access.[1202]

Thus, there are only two limited cases in the UK under which the blocking of Internet access and digital identity might legally occur: copyright infringement and specifically prescribed criminally illegal content. There is no general policy of State based blocking of public access to the Internet.

6.3.6.2.India

The Indian law and policy of blocking stands in vast contrast to the law and policy in the UK.

The Indian State is the main promoter and facilitator of digital technologies, particularly Internet access which is highly State regulated. In this sense, it assumes the mantle of gatekeeper of Internet access. It plays a significant role in determining access to digital identities, in manners far removed from that evident in the UK. [1203]

India has a history of blocking Internet access as a "balanced flow of information measure."[1204] This is evident in several examples. For instance, the blocking of access to the website of the Dawn newspaper in Pakistan during the Kargill war.[1205] In 2003, blocks were imposed on thousands of Yahoo! users by the Indian Computer Emergency Response Team (CERT-IN)[1206] under orders from the Department of

[1201] Hansard HC 'Offences Against Children: Internet,' col 692W (2 November 2009)
[1202] The Appeal Process is set out at <http://www.iwf.org.uk/corporate/page.49.625.htm>
[1203] A view reiterated by N Shah, 'Subject to Technology: Internet Pornography, Cyber-Terrorism and the Indian State,' (2007) 8 (3) Inter-Asia Cultural Studies, 349 - 366
[1204] Ministry of Communication and Information Technology (DIT), 'Order: Blocking of Websites,' 7 July 2003, New Delhi, Gazette of India, GSR 529(E), Extra, Pt II, S 3(i)
[1205] Farzad Damania, 'The Internet: Equalizer of Freedom of Speech? A Discussion on Freedom of Speech on the Internet in the United States and India,' (2002) 12 Ind Intl & Comp L Rev, 243
[1206] CERT-IN operates under the auspices of and with authority delegated by the Department of Information Technology, Ministry of Communications & Information Technology.

Telecommunications.[1207] Though the intent was to block a banned organisation from access,[1208] there was widespread denial of access to and use of Internet identities. When this action was taken it was severely criticised as having no legal basis under the ITA 2000,[1209] but the blocking was justified on the basis that it did not constitute a form of censorship, rather was conducive to the "balanced flow of information."[1210]

In another case, <www.hinduunity.org> was ordered to be blocked on 28 April 2004 by the Mumbai police on the grounds that it contained material that was of anti-Islamic nature.[1211] A community on Google's social networking service Orkut was blocked in Pune in June 2006 for "'objectionable and disparaging' comments against Great Maratha King Shivaji Maharaj."[1212] This action affected not only the Orkut community, but also other cybercafé users as police shut down cybercafés where users were found accessing Orkut. Similar action was taken again in 2006 - seventeen blogs were blocked and many blog services were disrupted for a long period of time.[1213]

The power to block digital identities (Internet based or otherwise) is explicitly supported by Section 69A of the ITA 2000 (as amended by ITAA 2008) which deals with the power to issue directions for blocking for public access of any information through any computer resource.[1214] The Central Government or its specially authorised Officer may by order direct any agency of the Government or

[1207] Vide Gazette Notification No GSR 181 (E) of 27 February 2003 & No GSR 529 (E) of 07 July 2003
[1208] Department of Telecommunications (LR Cell), 'Direction to Block Internet Website: "Groups.yahoo.com/groups/kynhun,' No. 820-1/2003-LR (Vol I)
[1209] S Dikshit, 'Bid to Block Anti-India Website Affects Users,' *The Hindu* (23 September 2003) <http://www.thehindu.com/2003/09/23/stories/2003092312761100.htm>
[1210] See Gazette Notification GSR 529 (E) of 7 July 2003.
[1211] Priya Ganapati, 'Mumbai Police Gag Hinduunity.org,' (May 2004) <http://us.rediff.com/news/2004/may/26hindu.htm>
[1212] PTI, 'Orkut Forum on Shivaji Maharaj Blocked,' (18 November 2006) <http://www.expressindia.com/fullstory.php?newsid=77287>
[1213] Department of Telecommunications (LR Cell), 'Direction to Block Internet Websites,' No. 820-1/04-LR, Vol-I <http://photos1.blogger.com/blogger/507/157/1600/Indian_censored_list.jpg>
[1214] While this section might be construed as blocking access to certain sites or resources, access to sites and platforms constitutes a means to digital identity and hence must be considered in this light.

intermediary[1215] to block access by the public to any information generated, transmitted, received, stored or hosted in any computer resource on the following grounds: the sovereignty and integrity of India, defence, security of the State, friendly relations with foreign States, public order or for preventing incitement to the commission of any cognizable offence[1216] relating to above. An intermediary who fails to comply with blocking directions can be punished with an imprisonment for a term which may extend to seven years and also be liable to fine. The reasons for the blocking order must be recorded in writing and the order must be subject to prescribed procedure and safeguards.

In this respect, Special Rules called the Information Technology (Procedures and Safeguards for Blocking of Access of Information by Public) Rules 2009[1217] make several provisions in respect of the blocking of information. Designated Officers (officer of the Central Government not below the rank of a Joint Secretary), may issue directions for blocking for access by the public any information generated, transmitted, received, stored or hosted in any computer resource under sub-section (2) of Section 69A of the Act.[1218] The Designated Officer, on receipt of any request from a Nodal Officer[1219] of an organisation or a competent court, may, by order direct any Agency of the Government or intermediary to block for access by the public any information or part thereof generated, transmitted, received, stored or hosted in any computer resource for any of the reasons specified in Section 69A (1) of the Act.[1220] There are also provisions for emergency blocking as an interim measure (in situations where delay is not acceptable).[1221]

[1215] An intermediary includes telecom service providers, network service providers, ISPs, web-hosting service providers, search engines, online payment sites, online-auction sites, online market places and cybercafés. S 2 (w), ITA 2000 (as amended ITAA 2008)
[1216] Defined in the CrPC 1973, S 2 (c) as an offence for which, a police officer may arrest without a warrant in accordance with the First Schedule or other in force.
[1217] Gazette of India, Extraordinary, Part II, Sec. 3(1) (27 October 2009)
[1218] Rule 3
[1219] Per Rule 4, every organisation must designate one of its officers as a Nodal Officer, notify the Department of Information Technology and publish the name of the Nodal Officer on its website.
[1220] Rule 5. For further procedure see Rules 6 (complaints procedure), 7 (examination of request), 8 (Complaints Committee) and 9 (emergency blocking)
[1221] Rule 9 (2)

What are Mahesh's rights in respect of a block imposed under Section 69A? Can Mahesh appeal against such a block imposed against his digital identity? There is no provision in the ITA 2000 (as amended by ITAA 2008) which gives Mahesh a right as a digital identity subject, to appeal against an order of blocking made by the State under Section 69A. Mahesh would have to challenge the block as unconstitutional under Article 19 (1) (a) of the Constitution which provides citizens with a right to freedom of speech and expression. However, if the State can prove that its actions fell within the scope of the exceptions in the Article,[1222] Mahesh would not have a remedy under the Constitution.

The government in India thus retains and exercises powerful control over access to digital identities vide the provisions of the IT Act 2000 (as amended by the ITAA 2008), as opposed to the UK. This control is perceptible in its ability to exercise unrestricted control over digital identity subjects by blocking public access to digital identity (and through penal provisions over failure to comply).

Countries thus have varying policies of blocking;[1223] States like India have a more tolerant policy of blocking,[1224] others like the UK, less so.[1225] These policies have a major impact on how and whether digital identity can be accessed and enjoyed.

[1222] Action taken in respect of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence. Art 19(2) of the Constitution.
[1223] R Deibert, J Palfrey, R Rohozinski and J Zittrain (eds), 'Access Denied: The Practice and Policy of Global Internet Filtering,' (2009) 52 (4) IEEE Transactions on Professional Communication PC, 413-415; 'Internet Censorship Increases: Which Countries Face Political Filters?' (2007) 258 PC Plus, 22; Clark Boyd 'Mapping Censorship,' (2007) 110 (5) Technology Review, 19
[1224] There is some international agreement about the need for access blocking in respect of child pornography. See Yaman Akdeniz, 'Governing pornography and child pornography on the Internet: The UK Approach,' (2001) 32 University of West Los Angeles L Rev, 247-275
[1225] For a critical analysis of Internet filtering regimes and technologies, see Ian Brown, 'Internet Filtering: Be Careful What You Ask For,' in S Kirca, L Hanson, (eds.), *Freedom and Prejudice: Approaches to Media and Culture* (Bahcesehir University Press, Istanbul 2008), 74-91; R Deibert, N Villeneuve, 'Firewalls and Power: An Overview of Global State Censorship of the Internet,' in M Klang and A Murray (eds), *Human Rights in the Digital Age* (GlassHouse, London 2005), 111-124

6.3.7. Control of personal data

Aarti Velumurugan is registered on the electoral register of her constituency. Her personal information such as her name, parentage, age, sex, home address and unique electoral identity number is made freely available in the online electoral register for her constituency on the Internet. Anyone may download, copy, print or sell this data. Aarti feels aggrieved.

The above case study focuses on digital identities in e-governance. E-governance is "a set of technology-mediated processes that are changing both the delivery of public services and the broader interactions between citizens and government."[1226] E-governance is a major generator and propagator of digital identities, in the UK[1227] and more particularly in India.[1228] This is because e-governance in India is seen as a means of improving delivery of and access to public services[1229] to "realise the basic needs of the common man."[1230] The State plays an active part in the creation and proliferation of e-governance based digital identities. The focus of this case study is one common form of such identity - electoral personal data.

6.3.7.1.UK

Is Aarti Velumurugan protected by law in respect of her personal information used for electoral purposes (electoral data)? The answer is in the affirmative.

[1226] Kate Oakley, 'What is E-Governance,' Resource Paper, (Council of Europe, 2003)

[1227] For analysis of e-government in UK see Helen Margetts, 'E-Government in Britain: A Decade On,' (2006) 59 (2) Parliamentary Affairs, 250-265; P Dunleavy, H Margetts, S Bastow and J Tinkler, 'New Public Management Is Dead: Long Live Digital-Era Governance,' (2006) 16 (3) J Public Adm Res Theory, 467-494; P Dunleavy and H Margetts, *Government on the Web 2*, HC 764, Session 2001-2002, (TSO, 2002); GM Lamb, *Computers in the Public Service* (Allen and Unwin, Sydney1973); H Margetts, *Information Technology in Government: Britain and America* (Taylor and Francis, 1999).

[1228] See P Gupta and RK Bagga, *Compendium of E-governance Initiatives in India* (Universities Press, India 2008), RP Sinha, *E-Governance in India: Initiatives and Issues* (Centre for Public Policy and Governance, New Delhi 2006), KN Agarwala and MD Tiwari, *IT and e-Governance in India* (Macmillan, Michigan 2002)

[1229] See Department of Information Technology, 'Government Notifications for Enabling e-Services' <http://mit.gov.in/content/government-notifications-enabling-e-services> E-governance infrastructure manifests in the State Wide Area Network (SWAN), State Data Centres (SDCs), National eGovernance Service Delivery Gateway (NSDG) and the Common Service Centres (CSC). E-governance services manifest in a range of services like commerce, pensions, income tax, immigration, central excise, elections, UID, e-courts, EDI, e-biz, land records, police, agriculture, e-districts, India Portal and State Portals.

[1230] Department of Information Technology, 'The National e-Governance Plan' <http://mit.gov.in/content/national-e-governance-plan>

Up to 2001, Electoral Registration Officers (ERO's) were obliged to disclose all electoral data upon payment of appropriate fee.[1231] But this position changed after *(Robertson) v Wakefield Metropolitan Council*.[1232] In this case, an objection was made to the sale of copies of the Electoral Register by ERO's to commercial companies. Kay, J ruled that the selling of electoral data to commercial concerns without opportunity for electors to object such uses of their data breached Article 3 of the First Protocol of the ECHR (right to free elections), Article 8 of the ECHR and Article 14(b) of the Data Protection Directive (right of data subject to object to the processing of personal data for direct marketing purposes).[1233] After *Robertson*, the Representation of the People (England and Wales) (Amendment) Regulations 2002 were passed which created two separate versions of the Electoral Register– the Full Register and the Edited Register.

The Full Register is a public document available for inspection only at registration areas in public libraries, council offices or at Electoral Registration Offices.[1234] The Edited Register is a version of the Full Register that is made available for sale excluding the names of electors wishing to protect their personal data and restrict junk mail (clear opt out). An electoral data subject in the UK has the choice of consenting to their electoral data being included in the edited version of the Electoral Register which can be offered for sale.

The Full Register is not available online, though the Edited Register can be obtained through online commercial organisations.[1235] The Full Register can only be inspected under supervision[1236] (to prevent unauthorised copying and theft).[1237] Copies are only supplied to certain specified people or agencies for certain specified purposes such as

[1231] Representation of the People Act 1983 (as amended by Representation of the People Act 2000), ss 9 to 13, as supplemented by Representation of the People (England and Wales) Regulations 2001 (SI 2001/No.341); Regs 48 and 49 and Representation of the People (England and Wales) (Amendment) Regulations 2001 SI 2001/No.1700
[1232] [2001] EHC Admin 915
[1233] S 11, DPA 1998
[1234] ICO Guidance suggests that ERO's are data controllers under DPA 1998. See ICO, 'Key Definitions of the Data Protection Act,' <http://www.ico.gov.uk/for_organisations/data_protection_guide/key_definitions_of_the_dpa.aspx>
[1235] See the Electoral Commission, 'Can I Search the Electoral Register Online?' <http://www.aboutmyvote.co.uk/faq/registering_to_vote/can_i_search_online.aspx>
[1236] Reg 43, RPR 2001
[1237] Reg 96, RPR 2001; Reg 95 RPR (Scotland) 2001

elections,[1238] the compilation of statistics,[1239] law enforcement[1240] and credit reference checking.[1241]

If a register is made available in digital form it has to be strictly protected against any copying, printing or transmission and making an allowance therein for a name based searches are strictly illegal.[1242] Only address based searches are permissible. Under the current data protection regime, ERO's are data controllers[1243] and they are obliged in the performance of their electoral legal duties (including the drawing up, maintaining and publishing of the Electoral Roll) to comply with the obligations imposed on them by the DPA 1998.[1244]

The importance of protecting personal data used for electoral purposes and made available online is brought out by enforcement notice served by the UK ICO on B4U Business Media Ltd under the DPA 1998 in 2006.[1245] The UK ICO had received 1,600 complaints about a website operated by B4U Business Media Ltd called <www.b4usearch.com> which permitted people to make searches of electoral roll data[1246] free of charge without any subscription or registration. The ICO found the company to be in breach of the first data protection principle[1247] as its use of the personal data was unfair, (since electors had the option since 2002 to opt out of being in the more public and accessible Edited Register), unwarranted and prejudicial to the rights and freedoms of the data subject's legitimate interests. The cessation of the online availability of the electoral data was ordered.

[1238] Regs 98, 100-106 and 108, RPR 2001; Regs 97, 99-105 and 107, RPR (Scotland) 2001; Scottish Parliament Order; NAW (RoP) Order 2007

[1239] Reg 99, RPR 2001; Reg 98, RPR (Scotland) 2001

[1240] Regs 107 and 109, RPR 2001; Regs 106 and 108, RPR (Scotland) 2001

[1241] Reg 114, RPR 2001; Reg 113, RPR (Scotland) 2001

[1242] Reg 43(1A), RPR 2001

[1243] A data controller is "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed." DPA 1998, s 1 (1)

[1244] These include complying with the data protection principles and the other provisions of the Act.

[1245] ICO, 'Information Commissioner's Office Finds Website in Data Protection Breach,' (4 July 2006), <http://www.ico.gov.uk/upload/documents/library/corporate/notices/b4u_enforcement_notice_130706.pdf>

[1246] The company was using pre-2002 electoral register information

[1247] This principle requires that personal data be processed fairly and lawfully and not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met. See Sch 1, Part I, (1) DPA 1998

This shows that there is a clear mandate that electoral data that is personal data, is of highly private nature and not something that is or ordinarily resides within the scope of the public domain. The privacy of electoral personal data must be respected and if breached may be successfully actioned under law.[1248] Aarti can invoke rights under the DPA 1998.

6.3.7.2.India

Is Aarti Velumurugan protected by law in respect of her electoral personal data in India, as in the UK? The answer is no.

Electoral rolls containing the names of registered voters[1249] are a crucial part of the election process in India and great attention is paid to their preparation and publication.[1250] These rolls are maintained by constituency and prepared under the superintendence, direction and control of the State Election Commission (SEC) by ERO's in accordance with the provisions of The Representation of the People Act 1950.

Every electoral roll generally has a title page (with year of preparation/revision, number, name, reservation status, extent of the constituency and the number of parts into which roll is divided), table of contents indicating in serial order the area covered by each part of the roll, followed by a constituency map. The roll contains individual elector details by household. The roll is published in draft form for inspection and copies (hard and soft) are supplied free of cost to every recognised political party in the state.[1251] After claims (e.g. in respect of omitted names and erroneous entries) and objections in respect of roll entries are attended to, inaccuracies are eliminated and corrections and revisions are made, the roll is finally

---

[1248] Richard Morgan and Ruth Boardman, *Data Protection Strategy: Implementing Data Protection Compliance* (Sweet and Maxwell, London 2003), 87-89

[1249] Per Art 326 of the Constitution, every Indian citizen, 18 years and above, is (if not disqualified on grounds of non-residence, unsoundness of mind, crime or corrupt or illegal practice) is entitled to be registered as a voter in India.

[1250] ECI, 'Handbook for Electoral Registration Officers,' (2008) <http://electionsgoa.nic.in/pdf/handbook_ero.pdf>

[1251] Rule 11 (c), RER 1960

re-published. It is distributed free of cost to every recognised political party of the state in hard and soft copies.[1252]

These electoral rolls are routinely published online by the SEC's in the following format:

111	EPIC NO. ATV1234567
Name: Aarti Velumurugan Father's Name: Thomas Velumurugan House Number: 110/4 Age: 31 Sex: Female	

Fig 6: Electoral Roll Data

The data in the rolls includes personal information like name, family, address, age and sex. In some cases, photographs are also included.[1253]

As at 7 July 2010, an online search facility for electoral personal data had also been made available by the SEC's. An example of how the search facility displays information is extracted below:

your constituency : CORTALIM

Assembly Constituency No :	27	*Part No :*	5
Serial No In Part :	635	*Section No in Part :*	2
Name :	**Rowena Rodrigues**		
Age :	**31**		
House No:	**355/7**		
Father/Husbad Name :	**Romelo Rodrigues**		
ID Card No :	**FXC1805092**		
Polling Station Name :	**Govt. Primary School, Sindole, Sancoale (Room No.2**		
Polling Station Area :	**Sindole**		

NOTE:- This Electoral search facility is provided for immediate/quick information to the public. Public are requested to verify the details with the original rolls avilable in the Taluka Offices.

Fig 7: Electoral Personal Data Obtained Through Search Request[1254]

[1252] Rule 22 (c), RER 1960
[1253] Merinews, 'Haryana Publishes Entire Voters Lists With Photo,' (3 March 2009) <http://www.merinews.com/article/haryana-publishes-entire-voters-lists-with-photo/15712414.shtml>
[1254] Retrieved from the online search facility of the Goa SEC (7 July 2010)

Electoral personal data, in India, thus resides ordinarily within the public domain, whether offline or online. It is easily accessible and there are no limits as to its accessibility, use and dissemination. In this sense, Aarti's electoral data becomes a worldwide public digital identity. As it stands, she has no control over the manner in which her digital electoral data is exhibited or used. The government and its agencies thus have a free rein in respect of the uses of data in e-governance contexts like elections.

Unlike the UK, there is no data protection provision under which Aarti can bring a claim either to restrict accessibility or the secondary use of her data. The limited data protection provisions in the IT Act 2000 (as amended by the ITAA 2008) do not apply. For e.g. section 43A (compensation for failure to protect data) does not apply because Aarti's information cannot be classed as sensitive personal information. Section 72 (breach of confidentiality and privacy) presupposes the existence of a contractual obligation between parties, and thus would necessitate an obligation of confidence which the SEC's under the current regime, seem not to owe to electoral data subjects.

Aarti cannot enforce a right to privacy in the data under Article 21 of the Constitution, because her electoral data is a matter of public record. This is in line with the reasoning in *Rajagopal,*[1255] *District Registrar and Collector v Canara Bank,*[1256] *Alika Khosla v Thomas Mathew*[1257] and *Khushwant Singh v Maneka Gandhi*.[1258]

This case study highlights how differences are clearly evident in how the law protects personal electoral data in the UK and India. While the law in the UK prevents personal electoral data from being publicly and freely available and thus subject to exploitation, the law shows no similar trend in India. This puts digital

[1255] **n722**
[1256] CA 6350-6374/1997 (SC)
[1257] (2002) 62 DRJ 851
[1258] AIR 2002 Del 58

identity subjects in the UK and India on unequal footing. While those in the UK have control over their electoral data, the digital identity subjects in India do not.

6.4. Analysis

The above exercise highlights how difference manifests itself in the applicatory aspects of the legal regulation of digital identity.

In case study 1 on the privacy of digital images, it was demonstrated how an individual digital identity subject in the UK has proven effective remedies in law for the violation of privacy, particularly in respect of publicly taken digital images. On the contrary, in India, an individual digital identity subject does not enjoy similar protection.

Case study 2, on sharing, demonstrated how the law in both UK and India imposes liabilities for harm resulting through the shared use of digital identities. While in the UK this is not so much of an issue, as sharing of digital identity technologies occurs to a greatly limited extent; it is a major problem in India, where sharing of technologies occurs on much larger and persistent scales. The law in India fails miserably to take into account these uses. Thus, is evident a mismatch between the law, the local context of digital identity and the *Volksgeist.*

Case study 3 on reputation highlights an interesting trend. In the UK, action for harm to online reputation comes across as individual based, grounded in civil litigation; in India, it is envisaged less as an individual's concern and more of State concern (collective interest) in the preference and wider use of criminal law.

Case Study 4 on anonymity demonstrates that the right to anonymity especially in respect of digital technologies in the UK is protected and facilitated by law. In India, there is no similar right to anonymity. The law in India, on the contrary, curtails and proscribes the use of anonymity in digital transactions. This is particularly evident in the elaborate legal conditions of identification established for public Internet use.

Case Study 5 on pseudonymity establishes how the use of pseudonymous digital identities is not per se illegal under the fraud law framework in the UK. Comparatively, the use of pseudonyms while technically not per se illegal in India is presumptively more conducive to attracting criminal sanctions for fraud.

Case Study 6 focussing on access to Internet resources, illustrates differences in the regulation of access to Internet resources in the UK and India. Limited powers and provisions exist and are exercised in respect of blocking of access to Internet resources in the UK with appropriate safeguards that protect individuals from arbitrary exercise of such powers. In India, the State exercises authoritative control over access to Internet resources and consequently, the access to and expression of Internet based digital identity, with little or no effective means for an individual to safeguard his rights.

Case Study 7 on the control of personal data epitomises how the legal treatment of personal data used in e-governance contexts (in this case, elections) varies from country to country. While digital identity subjects in the UK have established data protection rights in respect of their electoral data, digital identity subjects in India, have no parallel rights or protection.

There are two main issues arising out of this analysis: first, unequal status of digital identity subjects in the UK and India in respect of their digital identity; and two, the mismatch of the law, local conditions and the *Volksgeist* in India.

The Indian digital identity subject, as compared to its Western counterpart in the UK, is variantly regulated in relation to its digital identity. In effect, the Indian digital identity subject is rather inadequately protected in respect of its digital identity (particularly in relation to privacy, data protection) and has a much more constrained relationship with its digital identity (evident in access to digital identity, anonymity, pseudonymity, control of personal data). Therefore, digital identity subjects in UK and India are on unequal footing in respect of the regulation of their digital identity.

Most of India's laws that impact digital identity are of some foreign origin or as Watson states "borrowed" or "imitated."[1259] As outlined in Chapter 5, they do work well in most cases to regulate digital identity. However, this chapter shows how these laws create significant problems in terms of their mismatch with local conditions[1260] and the *Volksgeist.*

The *Volksgeist* is Savigny's "spirit of the people."[1261] Savigny visualised the law as a product of the people, their culture, and their daily lives.[1262] According to him, the law had to reflect the "unique needs and character of the people of each nation."[1263] Tilak too advocated this stream of legal thought in the context of India in proposing that law and legislation should take into account the local context of the people.[1264]

The failure to take into account local conditions[1265] and the *Volksgeist* is problematic. Law turns into a "misfit," or a "meaningless form of words."[1266] It is then not well received or even subject to rejection, particularly when it is not sufficiently localised. Law might also gradually breakdown when people being to work around it, making its efficacy suffer.[1267] Legal compliance is effected and enforcement becomes difficult.[1268] This is particularly exemplified in the case of the Indian ITA 2000

[1259] Watson (1974) **n50**

[1260] eg, the state of digital technologies (i.e. their operating conditions, penetration, access and use) and culture (ie, privacy, information sharing, communal use of personal information, attitudes to authentication and verification, anonymity and pseudonymity). See **Ch 3.**

[1261] Savigny famously stated, "Law . . . is first developed by custom and popular faith, next by judicial decisions-everywhere, therefore, by internal, silently operating powers, not by the arbitrary will of a law-giver." Hayward (1975) **n56**, 30

[1262] See Julius Stone*, Social Dimensions of Law and Justice* (SUP, 1966), 35-36

[1263] Luis Kutner, 'Legal Philosophers: Savigny: German Lawgiver,' (1972) 55 Marq L Rev, 280-296, 284; J Stone, *The Province and Function of Law: A Study in Jurisprudence* (HUP, 1946), 421-23

[1264] Sharma (2009) **n56**

[1265] Specifically substantiated at **6.3.2**. The law fails to consider India's peculiar socio-economic conditions in the use of and access to digital identity technologies. Gender, caste and class based inequalities in society fuel access, use and expression of digital identities. Also, privacy and information sharing norms affect and influence the treatment of digital identity.

[1266] Legrand (1997b) **n63,** 120

[1267] Take for instance, copyright infringement in India, which is open and widespread despite being illegal. People work around copyright law to access information and have a tolerant attitude to copyright violations. See Ministry of Human Resource Development, Government of India, 'Study on Copyright Piracy in India,' (1999) Ch VIII (enforcement & public awareness of copyright); R Vyas, 'Perfect Semblance: Imperfect Law,' *The Telegraph* (9 January 2009) <http://www.telegraphindia.com/1090109/jsp/opinion/story_10356023.jsp>; Rachana Desai, 'Copyright Infringement in the Indian Film Industry,' (2005) 7 Vand J Ent L & Prac, 259-278

[1268] Dalal (2007) **n57**; Rodrik (2007) **n57**

which though containing a substantial regime for the regulation of information technology fails in respect of its compliance and enforcement capacity.[1269]

6.5. Conclusion

The examination of the application of the law with the case studies in respect of key digital identity contexts demonstrate how differences exist in the application of the law regulating digital identity in the UK and India. These differences put digital identity subjects in the UK and India on unequal footing. The very legitimacy of many of the laws that exist and are being implemented in India is in doubt. There is also a strong mismatch between the law and the needs of Indian digital identity subjects. This calls for a looking at the situation afresh. Given that digital identity and its regulation have global and local dimensions, how can this challenge best be addressed? We next attempt to find this answer.

[1269] Pavan Duggal, 'Cyber-crime in India: The Legal Approach,' in Roderic Broadhurst and Peter Grabosky (eds), *Cyber-crime: The Challenge in Asia* (HKUP, HK 2005), 183-196; PT Joseph, *Ecommerce: An Indian Perspective* (Prentice-Hall, New Delhi 2006), 6

7. The regulatory future of digital identity: Examination of proposed legal solutions

> As soon as something is valuable and persistent, we seek to associate rights and duties with it. What will those rights be?
> -*Susan P Crawford*[1270]

7.1. Introduction

Research on the regulation of digital identity reveals various legal solutions advanced in respect of digital identity. These legal solutions can be classed into two broad groups: national legal proposals and transnational legal proposals. In the first category, fall the constitutional right to virtual personality (Costa Rica), the tort based right to identity (USA) and the right to database identity (UK). In the second category is a transnational solution - De Hert's right to identity.

This chapter examines these proposals in the light of the simultaneous globality and locality of digital identity and differences in its regulation. Are any, and if so which of these solutions best suited to take into account that digital identity and its legal regulation is subject to these conditions?

7.2. National legal proposals

This section examines some national proposals (in chronological order) made in relation to the legal regulation of digital identity. [1271] These are: the constitutional right to virtual personality (Costa Rica), the tort based right to digital identity (USA) and the right to database identity (UK).

[1270] Susan P Crawford, 'Who's In Charge of Who I Am? Identity and Law Online,' (2004) 49 NY L Sch L Rev, 211-229, 212

[1271] In addition to these, see NNG de Andrade, 'Right to Identity: The Foundations for a Renewed Legal Conceptualization,' 3rd International Conference on Computers, Privacy & Data Protection, Brussels (29-30 January 2010). Based on EU human rights law and the Italian right to personal identity, Andrade re-conceptualises the right to personal identity in the context of AmI with two elements: the right to multiple identities and right to be forgotten.

7.2.1. The constitutional right to virtual personality (Costa Rica)

The first proposal that came to the forefront in respect of the creation of specific right to digital identity was the attempt to create a specific constitutional right to virtual personality. In 2005, a Bill was introduced in the Congress of the Republic of Costa Rica[1272] by Congresswoman Marta Iris Zamora Castillo aimed at the enactment of a constitutional fundamental rights provision to protect the virtual personality.[1273] The Bill proposed the enactment of a new Article 24*bis* to the Political Constitution:

> Article 24 bis*:* Everyone has the right to have or not have a virtual personality, where one's presence, content and projection is regulated by each one of them. It may not be used for discriminatory purposes to the detriment of its holder. The State will guarantee that the information contained in a virtual personality will enjoy the appropriate technical and legal security, excluding non-authorized third parties that try to obtain it. The State may use the content of an individual's virtual personality, upon due authorization from the individuals themselves, as long as the purpose is for the benefit of the said individuals.[1274]

Virtual personality[1275] or *Personalidad virtual* is defined as the "the ubiquitous existence of an entity,"[1276] or the "virtual facets of a legal entity."[1277] In these respects, *Personalidad virtual* relates to digital identity and is acknowledged as equivalent to it.

[1272] Costa Rica is a constitutional democracy with a legal system based on the Spanish civil law system.

[1273] Congress of the Republic of Costa Rica, Constitutional Reform for the Protection of the Virtual Personality as a Fundamental Right, Law Bill, Congresswoman M I Zamora Castillo, Expedient No. 15890 (9 May 2005). Spanish version at <http://virtualrights.org/PROYECTO%20PERSONALIDAD%20VIRTUAL.doc>. As of March 2009, the Bill was with the Human Rights Commission.

[1274] Red IberoAmericana de Protection de Datos, Documentación, Republic of Costa Rica, <http://www.redipd.org/documentacion/legislacion/costarica-iden-idphp.php>. Alternate translation at A Guadamuz Gonzalez, 'Virtual Rights,' (14 November 2005) <http://technollama.blogspot.com/2005/11/virtual-rights.html>

[1275] The right draws from J Aizenman Leiner, 'Derecho Ubicuos o Virtuales,' <http:// www.virtualrights.org/ Derechos%20Ubicuos,>, 1

[1276] J Aizenman Leiner, JM Pedersen and Dr JM Rivero, 'Virtual Rights: Constituting a Global and Local Information Society,' v.0.9i (2003), <http://web.archive.org/web/20070221180059/virtualrights.org/files/project_overview_latest.pdf>, 2

[1277] FJ Campos Zamora, 'The Emergence of Virtual Entity as Positive Status Information,' <http://www.virtualrights.org/informaci.doc>

The Bill aims to protect the right to have (or not have) a virtual personality, to regulate such personality and protect it against third party abuse. It is intended to protect aspects of digital identity like presence, content and projection. Presence involves digital identity mediated inter alia on the computer/Internet (email, blogs, and social networks) telephone, mobile phones (SMS, MMS, voicemail) and other technologies like RFID. Content relates to data. Projection involves the manner of assertion of identity.[1278]

Additionally, the right to virtual personality aims at protecting the right to exist in cyberspace,[1279] visualised as an inclusionary right enabling freedom of expression and engagement in cyberspace. This freedom of expression and engagement manifests in the ability to access the Internet, have an email id, website or participate in other online activities.[1280]

The right to virtual personality, intended to be a fundamental constitutional right, aims at protecting the virtual presence of an individual. It also aims at protecting the right of free development and enjoyment of the virtual personality; evident in its intent to accommodate both cases of having and not having a virtual personality. It seeks to guard against any discrimination to the virtual personality and its bearer.

The right aims to put the individual, the subject of the virtual personality, in control of digital identity; though it does have a proviso that enables State based exploitation of the virtual personality provided consent has been obtained and if such use is in the interests of the person. In this connection, the State must guarantee that information included in the virtual personality has adequate legal and technical security. [1281]

[1278] eg, as occurring through Identity Rights Agreements or Link Contracts.
[1279] J Aizenman Leiner, '[OpenID] German Court Defines Fundamental Digital Privacy Right,' (15 March 2008) <http://lists.openid.net/pipermail/openid-general/2008-March/013823.html>
[1280] Aizenman Leiner (2003), **n1276,** 2, 4
[1281] J Aizenman Leiner, 'Communication to Yadis, IDGang and the VP Symposium' (3 March 2006) <http://lists.danga.com/pipermail/yadis/2006-March/002247.html>

The justifications for the proposed right are set out by Chinchilla Sandi.[1282] The right is deemed necessary to deal with the risks of the Information Society, to enable individuals fulfill their role as virtual persons through control over their *Personalidad virtual.* It is also deemed essential to promote e-participation, safeguard privacy and facilitate informational self-determination.[1283]

The right to virtual personality manifests as a constitutional fundamental right. In this sense, it seems to represent a powerful means of protecting one's digital identity through a medley of negative prohibitions, positive freedoms and limitations.

However, the right as a legal solution falls short in a number of respects. First, it pre-supposes that the digital identity subject is an autonomous individual capable of exercising free will and choice in the expression and control of his or her digital identities. Second, it problematically assumes that individual identity subjects want, choose and are able to control their digital identities.[1284] Third, it places upon the State a huge burden by laying on it the primary and ultimate responsibility for the protection of digital identity. The right does not recognise fully that digital identity regulation is, as previously demonstrated, a complex mesh of actors (individual, private and State). The combined role of these actors has largely been ignored (unless of course it is assumed that the State takes the full and final responsibility for actions of everybody, including itself). Finally, in totality it remains an individual-centric right. The right is constrained by these deficiencies.

7.2.2. The tort based right to digital identity (USA)

In 2008, Blackman proposed a tort based right to digital identity based on principles of US tort law, confidentiality and criminal law aimed at omniveillance (which per Blackman refers to all forms of "pervasive human monitoring" which results in

[1282] Carlos Chinchilla Sandi, 'Virtual Personality: The Need For Constitutional Reform,' (2005) 082 AR: Revista de Derecho Informático < http://www.alfa-redi.org/rdi-articulo.shtml?x=948>
[1283] Costa Ricans enjoy the right to informative self-determination (*derecho a la autodeterminación informativa*). See Resolution 14580-2006, Constitutional Court, Sentence 014580-2006; Constitutional Court, Sentence 014847-1999 and Constitutional Court, Sentence 754-2002
[1284] A problematic assumption as determined in **Ch 4 (4.7.5)**

threats to reputation, free speech and expression and personal safety) and specifically the distribution of personal digital images over the Internet.[1285]

Blackman weighs up the threat of omniveillance and argues (in the US context)[1286] that existing privacy torts like the public disclosure of private facts,[1287] intrusion upon seclusion,[1288] false light[1289] and appropriation[1290] are ineffectual in dealing with intrusive omniveillance technologies. This is for a number of reasons. First, the protections available under such torts are subject to restrictions which limit their scope.[1291] Second, when these torts were established, contemporary forms and levels of digital identity threats did not exist. Therefore, Blackman proposes a tort based right to digital identity that would enable a "workable equilibrium" between privacy and free speech and provide a remedy for victims of omniveillance.

Blackman's right to digital identity states,

> The right to your digital identity is violated when an individual or organization records and reproduces an image of another without consent using a visual or auditory enhancing device while
>
> (1) the party recorded possessed a reasonable expectation of privacy to not be recorded; (2) the matter recorded would be offensive to a reasonable person;
>
> (3) the recording is intentionally widely transferred or disseminated through any electronic medium to any electronic format; and
>
> (4) the recording is not newsworthy, where a newsworthy recording
>
> (4a) has social value,
>
> (4b) minimally intrudes into ostensibly private affairs, and

---

[1285] Josh Blackman, 'Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet,' (2008) 49 Santa Clara L Rev, 313-392

[1286] Per Blackman, there is a strong need for a new legal incentive to protect privacy in America. Blackman (2008) **n1285,** 353

[1287] Restatement (Second) of Torts § 652D (1977). The tort states: One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.

[1288] Restatement (Second) of Torts § 652B (1977). The tort states: [o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

[1289] Restatement (Second) of Torts § 652E (1977)

[1290] Restatement (Second) of Torts § 652C (1977)

[1291] Restatement (Second) of Torts § 652D Cmt. H (1977) & § 652B Cmt. C (1977)

(4c) the party that is recorded voluntarily acceded to the position of public notoriety.[1292]

The first element of the right is grounded in the tort of intrusion upon seclusion and draws from the jurisprudence of criminal law, media law and voyeurism statutes which take on nuanced and qualified views of privacy.[1293] The right abandons the traditional private public property distinction and focuses more on discerning whether an individual has a reasonable expectation of privacy.[1294]

The second element of the right prescribes that the violation must be "offensive to a reasonable person." Here Blackman departs from the prescription, under both the torts of public disclosure of private facts and tort of intrusion upon seclusion, that a violation in respect of them must be judged in the light of whether it is "highly offensive to a reasonable person," because these high standards are difficult to satisfy.[1295]

The third element prescribes that there must be wide transfer or dissemination over an electronic medium. A simple, purely personal transfer or limited dissemination does not come within the scope of the right. It is necessary that there is "indiscriminate dissemination to an electronic forum without concern for newsworthiness."[1296] Blackman quantifies transfer and dissemination in terms of whom the recording is released to and the distance it travels. The transfer and dissemination of the recording must be widespread and conducted proactively. The transferred recording must also be easily accessible and indefinitely retained.

[1292] Blackman (2008) **n1285**, 354-355

[1293] Citing *Katz v United States* 389 US 347, 360 (1967) (Harlan, J. concurring); *Olmstead v United States* 277 US 438, 464–65 (1928); *Sanders v ABC* 978 P.2d 67, 72 (Cal 1999)

[1294] What constitutes reasonable expectation of privacy was laid down in *Katz.* A reasonable expectation of privacy may be held to exist if a person has exhibited an actual (subjective) expectation of privacy and, second, the expectation is one society is prepared to recognize as reasonable. For detailed analysis of reasonable expectation of privacy in the US, see Robert Gellman, 'A General Survey of Video Surveillance Law in the United States,' in Sjaak Nouwt, BR de Vries and C Prins (eds), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (TMC Asser Press, Netherlands 2005), 7-35

[1295] *Tucker v Merck & Co* 2003 WL 25592785, at *13 (ED Pa 2 May 2003).

[1296] Blackman (2008) **n1285,** 365-366

The fourth element provides that the recording must not be newsworthy, to accord with rights under the First Amendment.[1297] Blackman here seeks to balance the social values of privacy and publicity. Newsworthiness is based on the three factored approach in the case of *Kapellas v Kofman,*[1298] where the California Supreme Court identified three important factors of newsworthiness:

> (1) the social value of the facts published
> (2) the depth of the article's intrusion into ostensibly private affairs, and
> (3) the extent to which the party voluntarily acceded to a position of public notoriety."

Blackman's right is strictly restricted in its remit; it does not include state based surveillance and matters under the Fourth Amendment of the US Constitution.[1299]

Blackman makes a lucid case for the creation of a tort based right to digital identity. One of the main advantages of his right is its specificity. It does not try to do too many things at one time. This it has achieved through restricting the remit of its operation. However, Blackman's proposal is extremely short sighted and flawed in one major respect. This relates to the fundamental grounding of the right in the need to protect identity through protecting privacy.

The problems of Blackman's approach can be gauged from the writings of Peek.[1300] Blackman presumes that there are two parties in the right to digital identity: one, who actively engages in privacy violating acts and the other, who has a reasonable expectation of privacy. Peek states that this is a 'flawed dichotomy' of privacy law because privacy law has and (even in Blackman's approach) fails to consider the fallout of the 'fluid, modern reality and concept' of the entities violating privacy and the entities having reasonable expectation of privacy 'mutually' engaging in such actions. Another reason Blackman's tort becomes hugely irrelevant is due to the

---

[1297] The First Amendment states: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.
[1298] *Kapellas v Kofman* 459 P2d 912, 922–24 (Cal 1969)
[1299] The Fourth Amendment relates to the right of persons against unreasonable searches and seizures.
[1300] Marcy Peek, 'The Observer and the Observed: Re-imagining Privacy Dichotomies in Information Privacy Law,' (2009) 8 (1) Nw J Tech & Intell Prop, 51-66

nature of the progress of technological innovations; technology often erodes into the expectations of privacy.[1301]

Blackman's right is predominated by the conceptualisation of a person's interest in privacy as a concern over 'accessibility to others.'[1302] But people do not always have an equal or universal interest in maintaining their privacy.[1303] Blackman problematically assumes that people constantly desire, prefer and act to preserve privacy. However, people often actively engage in acts that result in the violation of their own privacy.[1304] This is evident not just in the case of Indian digital identity subjects, whose digital identities are often of non-private and routinely shared natures, but also in respect of digital identity subjects in the West.

Blackman's proposal is further affected by its nature. Privacy torts are characterised as weak rights. In the US, courts have guardedly and rigidly interpreted these torts curtailing their scope as an effective remedy for rights violations.[1305] There are other reasons that make such torts ineffective. First, torts respond to intangible harms that are impossible to measure.[1306] Second, the resistance to dignity torts.[1307] Third, the complexity of pursuing such actions.[1308] If one adds to this the nature and lack of effectiveness of tort based remedies in India in protecting digital identity, it becomes clear that this solution is extremely limited in its effectiveness as an international

---

[1301] Paul M Schwartz, 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States,' (1995) 80 Iowa L Rev, 553- 618, 573. Also see **Chs 3 (3.2.2.1.1)** and **4 (4.7.2)**
[1302] See Ruth Gavison, 'Privacy and the Limits of Law,' (1980) 89 (3) The Yale LJ, 423
[1303] **Chs 3 (3.2.2.1), 4 (4.7.6)**
[1304] Lessig (2006) **n151**, 228; Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage Books, USA 2001); P Norberg, DR Horne and DA Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviours,' (2007) 41 (1) J Cons Aff, 100-126; Sarah Spiekermann, Jens Grossklags and Bettina Berendt, 'E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior,' in MP Wellman and Y Shoham (eds), *Proceedings of the 3rd ACM Conference on Electronic Commerce* (ACM, NY 2001), 38-47; Joseph Phelps, Glen Nowak and Elizabeth Ferrell, 'Privacy Concerns and Consumer Willingness to Provide Personal Information,'(2000) 19 J Pub Policy & Mktg, 27-41
[1305] DK Citron, 'Mainstreaming Privacy Torts' (2011) 99 California L Rev, 101-189
[1306] DL Zimmerman, 'Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort,' (1983) 68 Cornell L Rev, 291-367, 362
[1307] LB Lidsky, 'Prying, Spying and Lying: Intrusive Newsgathering and What the Law Should Do About It,' (1998) 73 Tul L Rev, 173-248, 211
[1308] RP Bezanson, G Cranberg and J Soloski, *Libel Law and the Press: Myth and Reality* (Free Press, NY 1987), 116 (success of privacy tort claims)

remedy. Therefore, the tort to digital identity, as proposed by Blackman is a highly limited solution.

7.2.3. The right to database identity (UK)

The right to database identity is propounded by Sullivan in her analysis of national ID schemes legislation (primarily the Identity Cards Act 2006 and the UK National Identity Scheme) in line with the "emergent legal concept of identity." [1309] Unlike Blackman, she opines identity is a better 'lens' than privacy to view digital identity problems.[1310]

The legal concept of identity, per Sullivan, includes two types of identity under the UK National Identity Scheme: database identity and token identity. Database identity includes "all the data and information recorded about an individual in the database/s accessible under the scheme."[1311] Token identity is "a subset of database identity and consists of name, gender, data and place of birth and death, signature, appearance (through comparison with a photograph) and biometrics."[1312]

Sullivan visualises the right to database identity as founded in the "broader right to identity under international law."[1313] She refers to the express declaration of the right to identity in Article 8 of the UN Convention on the Rights of the Child (UNCRC),[1314] the indirect references to identity in Articles 6 and 15 of the Universal Declaration of Human Rights (UDHR), the right to self-determination in Articles 1(2) and 55 of the UN Charter, Article 1 of the International Covenant on Civil and Political Rights (ICCPR) and Article 1 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) and the right to identity implicit in Article 8 of the ECHR. Sullivan finds that the basis of these rights is personal autonomy i.e. self-

[1309] Clare Sullivan, 'Privacy or Identity?' (2008) 2 (3) IJIPM, 289-324
[1310] A specific reference is made to identity theft, defined as "dishonest misuse by a person of another person's registered token identity for a transaction." See Sullivan (2009) **n7**
[1311] **n1309**, 290
[1312] ibid
[1313] Referring to international treaties and EC law.
[1314] Adopted and opened for signature, ratification and accession by GA Res 44/25 of 20 November 1989. E.i.f. 2 September 1990.

determination;[1315] the basis of which is the 'protection of the individual sector' and the 'zone of individual power,' both of which she argues are crucial for the "healthy development and functioning of the individual."[1316]

For grounding the right to database identity in 'identity' rather than privacy, Sullivan puts forth the following reasoning. Identity, she believes, is more essential,[1317] fundamental and absolute in comparison to privacy.[1318] It is better equipped to deal with identity abuses than privacy or data protection,[1319] goes deeper into the issue of control and thus, is a better medium to employ.[1320] Identity not only enables informational self-determination (which Sullivan appreciates as the primary role of privacy) but also the right of the individual to be recognised and protected as a unique individual.[1321]

The right to database identity is the right of an individual to:

1. an accurate, fully functional and registered identity i.e. his/her database identity including token identity;
2. Exclusive use of his/her transactional identity i.e. his/her token identity;
3. A right to know what information is recorded and to rectify errors
4. A right to know what information is disclosed and to whom"

The right to database identity highlights the importance of identity and disentangles it from privacy. In this sense it does substantiate the rationale that protecting digital identity is a not only limited or tied to the protection of privacy.

But there are problems with the arguments supporting the right. Though Sullivan prefers to focus and centres the right to database identity on identity rather than privacy, there is evidence of reluctance to make an effective leap from privacy to identity. This is evident in the manner Sullivan discusses the close relationship between the two.[1322] One cannot take this as a given, as the relationship between

---

[1315] **n1309**, 296
[1316] Referring to CA Reich, 'The Individual Sector,' (1991) 100 (5) Yale LJ, 1409-1448, 1442
[1317] **n1309**, 307
[1318] **n1309**, 299
[1319] **n1309**, 304, 305
[1320] **n1309**, 305
[1321] **n1309**, 307
[1322] **n1309**, 305

identity and privacy is highly contextual. Identity and privacy do not always share an intimate or coherent relationship. Moreover, identity and privacy do not share equal or similar relationships universally, particularly given local difference.[1323]

Another problem with the right to database identity is its nature. The right is, at best, a data protection right. This is because, the right in its different elements, particularly elements (3) and (4), is reflective of the principles of European (mainly, the EU Data Protection Directive) and UK data protection law (DPA 1998). For instance, the right to know what information is recorded (element 3) is grounded in Recitals 25, 30 of the Data Protection Directive and Section 7 (1) (a) of the DPA 1998 (right of access to personal data).[1324] The rectification of errors (element 4) is mirrored in Articles 10 (c) and 11 (c) of the Data Protection Directive and Sections 12,[1325] 12A[1326] and 14[1327] of the DPA 1998. The right to know what information is disclosed and to whom is enshrined in Recitals 30, 39 and Articles 11, 12 (a) of the Directive and Section 7 (1) (b) of the DPA 1998.

Even element (1) of the right to database identity is derived from data protection. The right to an accurate, fully functional and registered identity finds its roots in Recital 36 and Article 6 (d) of the Directive and Sections 12A (1)(a), 12A (5), 14(1) and the fourth data protection principle[1328] in Schedule 1, Part I of the DPA 1998. While data protection represents an important means of attaining informational self-determination, as desired by the right, data protection by itself has not and may not represent the best means of dealing with digital identity regulatory challenges.[1329]

[1323] **Ch 3 (3.2.2.1)**; **Ch 6 (6.3.1)**

[1324] This section states that an individual is entitled to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.

[1325] Rights in relation to automated decision-taking.

[1326] Rights of data subjects in relation to exempt manual data.

[1327] Rectification, blocking, erasure and destruction.

[1328] Personal data shall be accurate and, where necessary, kept up to date.

[1329] For instance, in jurisdictions with no or undeveloped data protection regimes. PM Schwartz, 'European Data Protection Law and Restrictions on International Data Flows,'(1995) 80 Iowa L Rev, 471-496; MD Kirby, 'Transborder Data Flows and the "Basic Rules" of Data Privacy,'(1980)16 Stan J Intl L, 27-66, 29; Hildebrandt (2008) **n173**, ss 15.5, 15.6; C Raab and Bert-Jaap Koops, 'Privacy Actors, Performances and the Future of Privacy Protection,' in Gutwirth and ors (2009) **n432,** 207-225, 216. For weakness of DPA 1998, see Great Britain Parliament House of Lords Select Committee on the Constitution, 'Surveillance: Citizens and the State,' 2nd Report of Session 2008-09, Vol 2, Evidence, House of Lords papers 18-II (2008-09), 125 (data processing), 396 (weak enforcement), 433 (surveillance); Aleksandra Kuczerawy, 'Facebook and its EU Users: Applicability of the EU Data Protection Law to US based SNS,' in M Bezzi and ors (eds), *Privacy and Identity,* IFIP AICT 300 (Springer, Germany 2010), 75-85

Yet another issue with the right relates to its intent to enable an individual have an "an accurate, fully functional and registered identity i.e. his/her database identity including token identity." The right to a registered identity has been in existence for a long time. International instruments like the UNCRC Article 7[1330] and national law provide for the right to registration. However, despite this right being guaranteed by law, its effectiveness is limited. It works better in countries with high levels of economic development and works less effectively or is rendered entirely meaningless to people in countries with low levels of economic development (and where civil registration infrastructure is either not well developed or fails to draw in the numbers). This can be substantiated by WHO figures on the registration of births and deaths,[1331] as well as UNICEF figures on regional disparities in unregistered births.[1332]

There are several challenges that may affect the right to enjoy "an accurate, fully functional and registered identity." Many of these relate to the structural design, application and implementation of the system in relation to which the right to identity is sought to be enjoyed. But the main concern relates to whether and how an individual will be empowered in the right to enjoy an accurate, fully functional and registered identity. An individual needs to be aware of the existence of such a right, the existence of inaccuracy or dysfunction in relation to his identity, must choose and be able to take actions to enforce the enjoyment of the right. This is an extremely difficult task as demonstrated by the case studies on sharing[1333] and electoral personal data,[1334] particularly when personal data is viewed as part of the collective commons in countries like India.

[1330] It states: "The child shall be registered immediately after birth and shall have the right from birth to a name [and] the right to acquire a nationality. . ."
[1331] Prasanta Mahapatra and ors, 'Civil Registration Systems and Vital Statistics: Successes and Missed Opportunities,' (29 October 2007) <https://www.who.int/healthinfo/statistics/WhoCounts2.pdf>
[1332] Per UNICEF, the highest number of unregistered births per year were in East/South Asia and Pacific, while the lowest number was in Europe and the Americas. UNICEF, 'Civil Rights Commentary,' <http://www.unicef.org/pon98/06-13.pdf>
[1333] **Ch 6 (6.3.2)**
[1334] **Ch 6 (6.3.7)**

The right to database identity is grounded in the pre-existence of an individual's fundamental human right to identity and self-determination.[1335] In its self-determinist nature, it reflects the Western individualistic liberal perception of an individual who is or must have full control of identity.[1336] But even in Western societies, this perception does not hold true for all purposes and accounts, particularly given that identity is often an associative and collective construct. It is even more inadequate for societies like India that openly reject the individualistic liberal perception of an individual's right to control their identity distanced from collectives of family, caste, kinship, religion or the State.

Sullivan visualises the right to identity as 'absolute,' one which is not "an individual right which is balanced against the public interest," and "can be never legitimately removed or unilaterally changed."[1337] The extent an unqualified, absolute right to identity, particularly in relation to database identity, would be accepted is highly debatable. To date, absolute rights are highly restricted. Even under the ECHR and the UK HRA 1998, few rights are absolute: right to life (Art 2), prohibition of torture (Art 3), prohibition of slavery and forced labour (Art 4), no punishment without law (Art 7), right to marry (Art 12), right to free elections (Art 3, First Protocol) and the right not to be condemned to a death penalty (Art 1, Sixth Protocol).

According to this, it can be concluded that Sullivan's right to database identity does not add much to the regulatory future of digital identity, and like Blackman's right is limited in its applicatory scope, given global implementation and local difference.

7.3. Transnational legal proposals

In addition to the national legal regulatory proposals, there are two international initiatives: first, the right to digital identity in the Charter of Human Rights and Principles for the Internet and second, the human right to identity proposed by Belgian academic Paul de Hert.[1338]

[1335] **n1309,** 305
[1336] See PM Schwartz, 'Beyond Lessig's Code for Internet Privacy: Cyberspace, Privacy Control and Fair Information Practices,' (2000) Wis L Rev 743
[1337] **n1309,** 309
[1338] De Hert (2007) **n76**

The Charter of Human Rights and Principles for the Internet[1339] drafted by the Internet Rights and Principles Dynamic Coalition (IRP DC) seeks to apply human rights standards and principles to the Internet. It is based on the UDHR and UN human rights law. It advocates: equal right to access to the Internet, right to freedom of expression, right to privacy, right to digital identity and right to data protection. The right to digital identity is co-opted under the right to privacy and provides that "everyone has a right to digital identity"[1340] The Charter is not examined in detail here because it in effect, it does not intend to create any new rights rather only "intends to layout and explain how existing agreed-upon human rights standards apply to the specific context of the Internet."[1341]

7.3.1. The right to identity

De Hert argues that a new human right to identity,[1342] in keeping with the trend of recognising individuals as legitimate and globally recognised rights holders and claimants in international and regional law and institutions,[1343] is necessary to protect the individual from technological threats particularly in the light of the resistance and lack of efficacy of the right to privacy.

De Hert's right to identity states,

> States Parties undertake to respect the right of each persons to preserve and develop his or her ipse and idem identity without unlawful interference.[1344]

This right is inspired and modelled on Article 8 of the UNCRC, which is the most unequivocal statement of a right to identity, available to children. The identity of a

---

[1339] The Charter is inspired by the Association for Progressive Communications (APC) Internet Rights Charter and builds on the WSIS Declaration of Principles of Geneva and the Tunis Agenda for the Information Society. <http://Internetrightsandprinciples.org/node/367>. For APC Internet Rights Charter, <http://www.apc.org/en/node/5677>

[1340] Charter, Principle 9 (b). Digital identity here refers to personal identification in information systems.

[1341] <http://Internetrightsandprinciples.org/node/367>

[1342] Prins similarly calls for a right to identity. JEJ Prins, 'Een Recht op Identiteit,' (2007) 82 (14) Nederlands Juristenblad, 849.

[1343] TM Franck, *The Empowered Self: Law and Society in the Age of Individualism* (OUP, Oxford 1999), 220

[1344] De Hert (2007) **n76**

child was deemed worthy of legal protection[1345] because of its ability to be in flux, which makes it vulnerable to being compromised or destroyed and international agreement was reached by delegates from countries representing different legal systems, values, and cultures on a right to identity for children. [1346] Article 8 states:

> 1. States Parties undertake to respect the right of the child to preserve his or her identity, including nationality, name and family relations as recognized by law without unlawful interference.
>
> 2. Where a child is illegally deprived of some or all of the elements of his or her identity, States Parties shall provide appropriate assistance and protection, with a view to re-establishing speedily his or her identity.

This Article was proposed by Argentina in the Working Group drafting the Convention with the intent of safeguarding identity interests of children through ensuring speedy intervention by the State in cases of violations against identity preservation.[1347] The background to this was that during the 1970's and 1980's when the Argentinean military junta was in power, there were a number of enforced and involuntary disappearances of people. Babies and children had disappeared, been killed or adopted by childless couples without any records and it was felt that something had to be done to find and establish the children's true identity.[1348]

Article 8 (1) of the UNCRC does not define "identity,"[1349] rather only mentions three elements of identity: name, nationality and family relations. But, these are not meant to be the only aspects of identity protected under this right as is evident by the use of

---

[1345] There is no parallel provision for adults.
[1346] In its Preamble the UNCRC states, "childhood is entitled to special care and assistance" and that "the child, by reason of his physical and mental immaturity, needs special safeguards and care, including appropriate legal protection, before as well as after birth" in synchrony with the Declaration of the Rights of the Child (1959) and asserts that "in all countries in the world, there are children living in exceptionally difficult conditions, and that such children need special consideration."
[1347] See UN Doc E/CN.4/1985/64 Annex II, p 1 at I. New Articles (Argentina)
[1348] E/CN.4/1986/39, 8-10; S Detrick, *The United Nations Convention on the Rights of the Child: A Guide to the Travaux Preparatoires* (Martinus Nijhoff, Dordrecht 1992), 292-294; The Declaration on the Protection of All Persons from Enforced Disappearance in 1992 (UN GA Res 47/133 of 18 December 1992) was adopted in this light.
[1349] D Hodgson, 'The International Legal Protection of the Child's Right to a Legal Identity and the Problem of Statelessness,' (1993) 7 (2) Intl J L and Family, 255-270, 265

the word "including" preceding these elements.[1350] However, in interpreting the elements of the right, the underlying guiding principle is the best interests of the child.[1351] Various aspects of identity are protected against unlawful interference by the Convention, e.g. Articles 2,[1352] 16,[1353] 20[1354] and 30.[1355]

7.3.1.1.Rational and nature

A right to identity is highly necessary, De Hert, argues for the age of the 'Internet of things.' The 'Internet of things' is the current and future technological age where technology is a pervasive and seamless part of life. According to an ITU report and Mark Weiser's vision, it is represented by the increasing availability of processing power accompanied by its decreasing visibility; a world of "anytime, any place connectivity for anyone," "connectivity for anything;" where technologies are "pervasive, interactive and intelligent." [1356]

In this setting, there arise various challenges to identity because of its play and performance at various levels: virtual communities, social networking, mobile technologies, RFID, chipped passports, ethnic screening, biomedical implants and AmI. Additionally, there is surveillance, identification, control schemes and profiling, all of which, according to De Hert, pose significant threats to the individual and society.

Examining case law under the ECHR, specifically Article 8, De Hert concludes that while certain identity aspects like name, gender and sexual orientation are afforded excellent protection in Europe, identity in relation to the Internet of things is not and thus there exists a gap in regulation. De Hert finds problematic the protection of identity through privacy law; this he opines is neither globally satisfactory nor does it

[1350] ibid. Other aspects of the identity subject to protection are the child's personal history since birth and race, culture, religion and language of the child. Rachel Hodgkin and Peter Newell, *Implementation Handbook for the Convention on the Rights of the Child* (UNICEF, 2002), 125
[1351] JS Cerda, 'The Draft Convention on the Rights of the Child: New Rights,' (1990) 12 HRQ, 115-119, 117
[1352] Right of child against discrimination.
[1353] Right to protection from interference with privacy, family, home and correspondence.
[1354] Special protection of child temporarily or permanently deprived of family environment.
[1355] Right of children of minority communities and indigenous populations to enjoy their own culture and to practice their own religion.
[1356] ITU, *Internet Reports 2005: The Internet of Things* (ITU, Geneva 2005), 2, 13

work well when weighed against interests like national security, public health and safety.

Therefore, to eliminate these problems De Hert proposes a new human right to identity with universal validity with the following aims and intents:[1357] One, to promote the enactment and effective implementation of procedural safeguards to protect the basic, inviolable rights of an individual to his identity. Two, to limit the formal denigration of individual rights and liberties. Three, to protect individuals against risks of technology abuse. Four, to protect human rights against widespread global technological surveillance and profiling.[1358] Five, to deal with the lack of human intervention, knowledge and control in identification processes.[1359] Six, to fulfil the need for "explicitness" and "awareness" of identity rights. Seven, to realise the balance between the rights of individuals and the public interest.[1360]

So, what constitutes De Hert's right to identity? What are its key elements? What is its scope and effect, and how best does De Hert fill the regulatory gap?

7.3.1.2.Key elements

The right to identity comprises of the following elements: a positive obligation on State Parties, preservation and development of ipse and idem identity and a right against unlawful interference.

7.3.1.2.1. Positive obligation on state parties

As opposed to the right to privacy, which is typically understood as a negative right,[1361] De Hert argues for a positive right to identity.[1362] A positive right is a right that entitles its holder to be provided with the conditions under which its fulfilment is

[1357] De Hert (2007) **n76**
[1358] Hildebrandt (2008) **n173**
[1359] ibid
[1360] GJ Walters, *Human Rights in an Information Age: A Philosophical Analysis* (University of Toronto Press, Toronto 2001),187
[1361] See Louis Brandeis, 'The Right to Privacy,' (1890) 4 HLR, 193-220, 216; SJ Sucher**,** *The Moral Leader: Challenges, Tools and Insights* (Routledge, US 2007), 198; BW Schermer, *Software Agents, Surveillance and the Right to Privacy: A Legislative Framework for Agent-enabled Surveillance* (Amsterdam University Press, Amsterdam 2007), 118. Also evident in its being legislated as a negative right in Art 12 UDHR and the negative liberty approach in Art 8, ECHR.
[1362] Citing Hildebrandt (2008) **n173**

achieved. A negative right on the other hand, merely implies that the right holder is entitled to enjoy such a right without interference.[1363]

De Hert frames the right to identity primarily as a positive obligation upon contracting State Parties[1364] that requires the taking of appropriate measures to ensure that individuals enjoy their rights.[1365] As such, States would be required to ensure the effective enjoyment of the right. For instance, through amending laws to conform to the obligations of the right, or establishing and facilitating the use of and access to services such that the right to identity could be enjoyed e.g. not arbitrarily blocking public access to Internet services or providing free user accounts to people to use crucial services.

Positive obligations under the ECHR entail the following: enabling the creation of a legal framework that would deter the infringement of a right,[1366] taking measures to protect persons at risk from right violations either from the State or third parties,[1367] providing information and advice,[1368] establishing effective judicial system for redress,[1369] investigating claims of violations,[1370] and ensuring fairness of procedure

[1363] This distinction is rejected by Holmes and Sunstein who state that, "all legal rights are, or aspire to be, welfare rights." (welfare as synonymous with positive rights). Stephen Holmes and CR Sunstein, *The Cost of Rights: Why Liberty Depends on Taxes* (WW Norton & Co, NY 1999), 222

[1364] De Hert's right while primarily shrouded with a positive nature, desires also to incorporate the negative element. He states that "identity needs to be understood in dynamic terms, necessitating a mix of negative and positive freedom." De Hert (2007) **n76**, 10, 13

[1365] See *August v UK* (2003) 36 EHRR CD 115, *Ivison v UK* (2002) 35 EHRR CD 20, *Stubbings v UK* (1996) 23 EHRR 213, *Deep Vein Thrombosis* (2002) EWCH 2825 (QB), *X & Y v Netherlands* (1985) 8 EHRR 235

[1366] *Tarariyeva v Russia*, EctHR, App 4353/03 (14 December 2006), para 74 (Article 2); *Storck v Germany* (2005) 43 EHRR 96, paras 149-152 (Article 5); *Őneryildiz v. Turkey* (2004) 39 EHRR 12, paras 89-90; *MC v Bulgaria*, [2003] ECHR 646, para 149; *Edwards v United Kingdom* (2002) 35 EHRR 19, para 54; *Osman v United Kingdom*, (2000) 29 EHRR 245, para 115; *Z v the United Kingdom*, [2001] 2 FLR 612 paras 73-75 (Article 3); *A v United Kingdom*, (1999) 27 EHRR 611, para 22; see also *X & Y v Netherlands* (1985) 8 EHRR 235, para 27; *Airey v Ireland* (1979) 2 EHRR 305, para 32 (Article 8)

[1367] *MC case,* para 152 (Article 3); *Osman,* para 115; *Keenan v United Kingdom* (2001) 33 EHRR 913, para 90; *Edwards*, para 54 (Article 2); *Menson v UK* (2003) 37 EHRR CD 220

[1368] *Őneryildiz,* para 90; *Guerra v Italy* (1998) 26 EHRR 357 (Article 8, obligation to provide information to those at risk of environmental pollution); *LCB v United Kingdom* (1999) 27 EHRR 212 (Article 2, obligation to provide information to those affected by nuclear testing)

[1369] *X & Y,* para 27 (Article 3); *Edwards,* para 54; *Vo v France*, paras 90-91; *Tarariyeva*, para 75 (Article 2)

[1370] *Jordan v United Kingdom* (2003) 37 EHRR 2, para 109 (Article 2 case); *MC case*, para 151; *Assenov v Bulgaria* para 102 (Article 3) *Akdeniz v Turkey*, EctHR, App 25165/94 (31 May 2001), (duty to investigate disappearances).

in interferences with qualified rights.[1371] Positive obligations are thus, meant to play a practical and effective role and not just be 'theoretical and illusory.' [1372]

While positive obligations bind, States generally enjoy a wide margin of appreciation in making a decision on the manner in which they will implement such obligations[1373] in international human rights law.[1374] This factor will determine the effectiveness of the right to identity.

7.3.1.2.2. Preservation and development of identity

The right to identity speaks of the preservation and development of identity. To preserve one's identity means taking any of these steps in respect of identity e.g. protecting or defending one's name, sexual identity, maintaining cultural identity, image and likeness, nationality, family identity etc. Preserving one's digital identity might mean protecting digital reputation, securing digital identities and controlling the processing and sharing of personal data. Developing one's digital identity might mean creating an email id, building up a social networking profile, changing a user name or other digital identity attributes or upgrading digital identities.

De Hert does not outline what 'preserve' and 'develop' under his proposed right to identity means. But as discussed in the preceding part, the preservation and development of identity could extend to any of the following: protecting and maintaining identity; being able to make choices about identity being able to create, change, use, propagate, share or destroy; being able to have an identity or a right not to be deprived of identity.

[1371] *TP v United Kingdom* (2002) 34 EHRR 2, para 72; *Hatton v United Kingdom* (2003) 37 EHRR 611 paras 99, 104

[1372] Citing *Dodov v Bulgaria*, EctHR, App 59548/00 (17 January 2008), para 83; *Őneryildiz,* para 69; *Ilhan v Turkey*, EctHR, App 22277/93 (18 May 2000), para 91; *X and Y v Netherlands* (1985) 8 EHRR 235, para 23; *Platform*, para 32; *Artico v Italy,* (1980) 3 EHRR 1; *Steel & Morris v United Kingdom* (2005) 41 EHRR 22

[1373] In the UK, it has been held that a treaty is not part of law unless it is incorporated into the law by legislation. *R v Lyons* (2002) UKHL 44 per Lord Bingham; *JH Rayner Ltd. v Dept. of Trade & Industry* (1990) 2 AC 418 HL at 500C per Lord Oliver of Alymerton.

[1374] *Abdulaziz, Cabales & Balkandali v UK* (1985) 7 EHRR 471, para 67; *Winer v UK* 48 DR 154 (1986); *Buckley v UK* (1996) 23 EHRR 101

While no international legal instrument (other than the UNCRC) specifically provides a right to preserve and develop identity, some approximating elements can be found in some international instruments like the 1948 Convention on the Prevention and Punishment of the Crime of Genocide[1375] and the Declaration on the Protection of All Persons from Enforced Disappearance.[1376] Under the UNCRC, "preserve" means non-interference in identity and maintenance of identity records and their confidentiality because such records are held to be of great significance in enjoying legal rights. A right to preserve might entail penalties for breaches.

The preservation of diverse aspects of an individual's identity is a strong premise that emerges from the jurisprudence of Article 8 of the ECHR,[1377] which has been interpreted to protect "a right to identity and personal development."[1378] Under this regime, the ECtHR in *S and Marper v the United Kingdom,*[1379] stressed the relevance of an individual's right to preserve his/her identity and confirmed that States were to ensure that appropriate safeguards existed under domestic law to enable the preservation and development of identity particularly in cases of automatic data processing and data with long life duration to prevent misuse and abuse.[1380]

Under De Hert's right to identity, States would thus incur a positive obligation to promote the preservation and development of digital identities. They would be obliged to ensure that digital identity was secured by means of appropriate technological infrastructure and legal measures.

[1375] Adopted by UN GA Res 260 (III) A on 9 December 1948. The words 'preserve and develop' are not specifically mentioned, but the spirit of the Convention resolutely promotes the preservation and development of identity.
[1376] **n1348**
[1377] See **Ch 5 (5.2.2.1.1)**
[1378] *Bensaid v UK,* ECtHR, App 44599/98 (6 February 2001)
[1379] [2008] ECHR 1581. The case was brought against the UK by the applicants in relation to the ongoing retention of their fingerprints, cellular samples and DNA profiles on the England and Wales National DNA Database even though they had been acquitted/or criminal proceedings against them had been discontinued.
[1380] para 103

7.3.1.2.3. *Ipse* and *idem* identity

An important aspect of De Hert's approach is the inclusion of the concepts of *ipse* and *idem* identity (as developed by Ricoeur[1381] and highlighted by Hildebrandt)[1382] in the right to identity, as a reminder of the complexity of identity.

Ricoeur developed the theory of identity in his book "Oneself as Another," where he identified five essentials - language, history, time, space and body - as the determinants of identity. Per Ricoeur, identity is both a stable and unstable concept; and it is in this context that his distinction between *ipse* and *idem* identity becomes important. *Ipse* identity connotes 'selfhood;' *idem* identity stands for 'sameness.'

Ricoeur explains *ipse* identity thus: "identity in the sense of *ipse* implies no assertion concerning some unchanging core of the personality."[1383] It is the dynamic, changing element of identity. As for the *idem* identity, Ricoeur maintains that,

> ..identity in the sense of the idem unfolds an entire hierarchy of significations (…). In this hierarchy, permanence in time constitutes the highest order, to which will be opposed that which differs, in the sense of changing or variable.[1384]

Idem identity is thus the underlying, unchanging reality of identity.

Both concepts are interactive and correlated, may overlap or exist in completely different zones. De Hert sums it thus:

> Personal identity is understood as a mix of *ipse* identity and *idem* identity. *Ipse* (or self) identity is the irreducible sense of self of a human person. It is reflexive consciousness of oneself. *Idem* (or sameness) identity is the objectification of the self that stems from comparative categorisation.[1385] Elements of *idem* identity are social identity, cultural identity, legal identity ('identité civile').

[1381] Kathleen Blamey (tr), *Paul Ricoeur, Oneself as Another* (Chicago U Press, Chicago 1992)
[1382] Hildebrandt (2008) **n173**
[1383] Blamey (1992) **n1381,** 2
[1384] Blamey (1992) **n1381**
[1385] David Pellauer (tr), *Paul Ricoeur, The Course of Recognition* (HUP, Harvard 2005); Hildebrandt (2008) **n173**

Therefore,

Personal identity	= *ipse* + *idem* identity.
Ipse identity	= self identity (irreducible/reflexive consciousness of self)
Idem identity	= objectified (comparative) self identity

Thus, *ipse* identity is a first person identity construct while *idem* identity is based on ascription by third persons. However, it is important to remember that both are intricately linked and only mutually of significance to the individual.

7.3.1.2.4. Right against unlawful interference

The phrase "without unlawful interference" forms the crux of the character of the right to identity and qualifies it.[1386] However, De Hert does not comment on what constitutes an 'unlawful interference.'

Unlawful interference[1387] may signify many things: an interference or intervention that is arbitrary, not prescribed by law or contrary to law. It could also mean an interference that is not in accordance with law, not proportionate or justified, as mandated to be. A number of international legislative instruments provide direction on what constitutes an unlawful interference.

In the UDHR, interference is referred to in Article 12,[1388] which states that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation and that everyone has the right to the protection of the law against such interference or attacks. Rather than unlawful interference, the Declaration mentions arbitrary interference, which is to be taken as meaning "not in accordance with well established legal principles."[1389] But the arbitrary element in the UDHR was intended to have specific limited range and

[1386] The qualification of rights is not unique to the right to identity and is a common occurrence in human rights law e.g. Articles 8-10 of the ECHR. See R English and P Havers (QC), *An Introduction to Human Rights and the Common Law* (Hart, Oxford 2000), 19

[1387] Interference, by itself, refers to an act or instance of meddling, prying, intrusion, hindrance, intervention, obstruction or impediment.

[1388] Cited here for its relevance to the regulation of digital identity.

[1389] See Johannes Morsink, *The Universal Declaration of Human Rights: Origins, Drafting, and Intent* (Uni of Pennsylvania Press, Pennsylvania 2000), 138

may not be the best guide to interpret what unlawful interference in the context of De Hert's right to identity. So, we must look to other legal instruments for guidance. In the ICCPR, Article 17 guarantees protection of law to privacy family, home, correspondence, honour and reputation, from arbitrary and unlawful interference.[1390] The travaux préparatoires of the ICCPR reveal great discussion about the meaning and scope of the terms arbitrary and unlawful interference.[1391] Issues were raised in respect of the applicability of the provision -whether it sought to protect individuals solely from the acts of public authorities or also against private persons. It was expressed that it should apply to only governmental action with the activities of individuals to be left to municipal legislation.[1392]

The UN General Comment on Article 17[1393] discussed arbitrary and unlawful interference and made several points. One, that interference could arise from state authorities, natural or legal persons.[1394] Two, that 'unlawful' should be interpreted to mean there was to be no interference except under circumstances envisaged by the law.[1395] Three, any interference authorised by States could only take place on the basis of law, which itself had to comply with the provisions, aims and objectives of the Covenant.[1396] Four, 'arbitrary interference' could extend to interference provided for under the law. Five, interference to escape the scope of the Article had to be reasonable under the circumstances.[1397]

Since, De Hert's right to identity was inspired by the UNCRC; it might be the most appropriate place to get guidance on the term "without unlawful interference." This term was much deliberated in discussions prior to the adoption of the UNCRC.

[1390] For interpretation see the Human Rights Committee General Comment 16(1988); UN Doc A4625/section 39

[1391] Commission on Human Rights, 9th Session (1953), A/2929 Ch VI, §100-102; Third Committee 15th Session, (1960), A/4625, § 36

[1392] E/CN.4 SR 374 pp. 4-5 (USA); E/CN.4 SR 375, p 8 (GB & AUS)

[1393] UN General Comment No. 16, 'Article 17 (Right To Privacy),' Thirty-Second Session (1988), Compilation of General Comments and General Recommendations Adopted By Human Rights Treaty Bodies, HRI/GEN/1/Rev.7 (12 May 2004)

[1394] UN General comment No. 16, para 1

[1395] UN General comment No. 16, para 3; A Conte, 'Privacy, Honour and Reputation,' in A Conte, S Davidson and R Burchill (eds), *Defining Civil and Political Rights: The Jurisprudence of the United Nations Human Rights Committee* (Ashgate, Aldershot 2004), 145-160, 147

[1396] UN General Comment No. 16, para 3

[1397] UN General Comment No. 16, para 4

Guidance on the interpretation of the UNCRC suggests what constitutes unlawful interference (in relation to identity aspects like race, culture and religion):[1398] suppression of minority languages in educational system, state information and the media; state persecution or proscription of the practice of a religion and failure to give adopted, fostered or institutionally placed children the chance to enjoy their ethnic, cultural, linguistic or religious heritage.

Thus, there can be a broad or limited ambit to unlawful interference depending on the context. Unfortunately, De Hert's right to identity does not make very clear its ambit and scope in relation to digital identity, though it is possible that the right could be sought to be applied in relation to the case studies discussed earlier.

7.3.1.3. Appraisal of the right

Is De Hert justified in proposing a new human right to identity? To a considerable extent the conclusion that this thesis reached is in the affirmative. Especially for countries like India, classical rights like privacy cannot fully capture the more pressing legal identity issues that beset it e.g. access to, establishment and enjoyment of digital identity.

On the other hand, De Hert himself recognises that "a general right to identity may not achieve the delicate balancing of interests needed to pay justice to any single, specific as well as contingent and contextual claim to identity."[1399] He recognises that the right may have undesirable consequences in terms of the "clamour for recognition and respect" of various other identity categories, many of which are strikingly troublesome and fraught with consequences; that it may "ignite sensibilities which are already overstretched"[1400] and that it may "heighten the tension between personal and collective identities."[1401]

[1398] Hodgkin (2002) **n1350,** 125
[1399] De Hert (2007) **n76**
[1400] Referring to E Balibar & I Wallerstein (eds) *Race, Nation, Class: Ambiguous Identities* (Verso, London 1991); S Huntington, *The Clash of Civilizations and the Remaking of World Order* (Simon and Schuster, NY 1996)
[1401] De Hert (2007) **n76**

De Hert's right to identity has been critiqued by Gutwirth who advocates the need to move beyond identity in the world of the Internet of things, AmI, profiling and control.[1402] While Gutwirth views De Hert's formulation of the right to identity as complementary to the development of a right to identity in European jurisprudence particularly Article 8 of the ECHR, he outlines a number of problems with it.

Firstly, Gutwirth builds the case that identity is a fundamentally flawed, problematic and controversial concept; as evident in clashes between individual and group claims. He distinguishes between a right to identity and the need of individuals to be protected against group based identities, unless they have made a choice to identify themselves with that group (using the opt-in, opt-out example). Here Gutwirth makes a broad assumption that "groups do not pre-exist as persistent entities that remain identical but on the contrary… are willingly constituted by their individuals, and they are permanently in a state of flux;" showing Gutwirth's predilection for the Western individualised concept of identity.[1403] However, as the analysis throughout the thesis has shown, this conclusion is unwarranted. While identity is a difficult concept, it is useful, manageable and can be sufficiently responsive to cultural differences.

Secondly, Gutwirth believes that identity at the individual level is an ever changing absurdity and prefers that identity not be referred to as something that defines a person or entity, rather, as a process of "belonging" or "becoming" (in line with Deleuze[1404]and Stengers).[1405]Again, this is something that does not fundamentally affect the right to identity as proposed by De Hert and which our analysis has shown can be accommodated within identity discourses.

Gutwirth also raises the issue of technical problems. He believes that the right to identity is subjective and open to interpretational difficulties.[1406] These difficulties relate to how identity is defined or described, what forms of identity are subject to

[1402] Serge Gutwirth, 'Beyond Identity?' (2009) 1 (1) IDIS, 123-133
[1403] Gutwirth favours a deconstruction that primarily focuses on individuality.
[1404] Gilles Deleuze, 'Contrôle et Devenir' and 'Post-Scriptum sur les Sociétés de Contrôle' in *Pourparlers 1972–1990* (Minuit, Paris 2003), Chs 16, 17
[1405] Isabelle Stengers, *La Vierge et le Neutrino* (Les Empêcheurs de Penser en Rond, Paris 2006)
[1406] Acknowledged by De Hert.

protection and what forms are not. Identity, as demonstrated before, is fraught with cross cultural legal, terminological and difference. So is digital identity, as demonstrated by the preceding chapters of the thesis. While De Hert's analysis does not take this explicitly into account or address it effectively, this thesis has argued, and substantiates that consistent extensions of his notion that accommodate this insight are not only possible, but indeed sympathetic to his core concerns.

Making distinctions in identity might be problematic - as evidenced in the discussions and in the *travaux preparatoires* of the UNCRC. Different countries had different 'identity' aspects included expressly in the right to identity while others had entirely different views.[1407] Detrick reports this in great detail.[1408] Some countries like Canada brought up how their jurisdictions did not recognise the identity concept, others raised concerns of its unacceptability.[1409] But in our framework, this is only to be expected. Paradoxically, identity needs not be identical across all contexts. Just as http protocols allow communication between very different computer systems using different computer languages; law's abstract, conceptual framework allows translation between different identity conceptions that while distorting, like every translation, parts of the local meanings are sufficiently robust to allow communication. Here, law and legal solutions score over Lessig's regulation by architecture,[1410] as argued in the analysis of identity management.

Gutwirth's sharpest criticism is encapsulated by the statement that a right to identity is "the best way to kill identity as a dynamic, open complex process…"[1411] Gutwirth seeks rather to maintain the status quo and advocates that identity issues be protected by "normative prohibitions of interferences such as foreseen by privacy and some aspects of data protection law"[1412] and other rights like freedom of conscience, speech and physical integrity. This is problematic because privacy and data

[1407] Hodgkin (2002) **n1350**, 384; see positions of Poland, Netherlands, US, Canada and Austria.
[1408] Sharon Detrick, *A Commentary on the United Nations Convention on the Rights of the Child*, (Martinus Nijhoff, The Hague 1999), 160-161
[1409] See UN Doc. E/CN.4/1986/39, paras 37, 44, 46
[1410] Lessig (1999) **n655**
[1411] Gutwirth (2009) **n1402**
[1412] Citing De Hert and Gutwirth.

protection as demonstrated before are subject to local difference and do not work in all circumstances to protect digital identity.

As to identity related claims Gutwirth suggests that these be dealt with under positive obligations of the states and judicial interpretations of the right to self-determination and autonomy. Where this falls short, legislators could be left to rise to the occasion and topically intervene.[1413] But this takes one back to square one where the identity is wedded to and enamoured with privacy and informational self-determination, which as has been shown before is a highly unsatisfactory state of affairs, given that privacy and data protection (law and practice) have proved highly inefficient in protecting the interests of the digital identity subject, particularly in countries like India that do not subscribe in *toto* to the Western nature of these values.

In the light of this thesis, there are other issues that present themselves in respect of the right to identity. These are advanced below.

7.3.1.3.1. The problem of the *ipse-idem* terminology

Firstly, there is the problem of the *ipse/idem* terminology. While categorising identity into *ipse* and *idem* identity lends much to the discourse, it does represent a problem, in respect of the international relevance of these terms in jurisdictions beyond which they were developed. Not everybody would be able to relate to identity in terms of the *ipse* and the *idem.*[1414] People in different parts of the world conceptualise identity differently, and may seek different frameworks for identity, one that is locally relevant. But given that digital identity has both global and local natures, the challenge is to have a universally valid and yet locally acceptable framework.

7.3.1.3.2. Individualist orientation

Even though the right to identity aims to be a balanced solution (with positive and negative elements), at its heart, it retains a strong Western individualist orientation

[1413] This presumes that legislators are aware and willing to act on a matter.
[1414] See **Ch 2 (2.2**) (cross cultural terminological differences in identity)

deeply rooted in individual autonomy.[1415] This is evident in the manner De Hert speaks of "threats to the individual," "the right to self-determination of the individual," "individual's claim for freedom in making choices about his or her own life," "reconstruction of one's identity… is just as we breathe, feel or think."

Though De Hert acknowledges the relevance of different perspectives to identity, the language and rationale for the right seems weighted down in favour of the atomic individual or the digital identity subject who seeks at all times to be in control of his digital identity. This might lend itself then to the criticism that Marx made of individualist rights based approaches: that these were too individualistic, egoistic and selfish i.e. an individual with rights was an "isolated nomad…withdrawn behind his private interests and whims and separated from the community."[1416] This also does not bode well for jurisdictions like India, where society and law does not perceive the individual primarily as atomic rather as an individual tied to the collective, be it the family, caste, or State and expressing rights primarily in such settings.

Instead, we must not give up on the concept of identity; rather recast it as a relational concept. Identity is (also) the sum total of an individual's relations and connections, an approach close to the Indian 'collectivist' mentality, and also widely evident in the thriving social networking context (representing interlinked identities).[1417]

[1415] Of the nature of Dumont's *Homo Aequalis,* represented by self-contained, self-interested individuals. The analysis in the thesis has highlighted how India's digital identity subjects do not fit into this category, rather fit within the category of *Homo Heirarchicus*, represented by individuals of traditional societies like Indian where "relations between men are more important, more highly valued, than the relations between men and things." Louis Dumont, *From Mandeville to Marx: the Genesis and Triumph of Economic Ideology* (Univ. of Chicago Press, Chicago 1977), 5; Louis Dumont, *Homo Aequalis* (Galliamard, Paris 1977); Louis Dumont, *Homo Hierarchicus: the Caste System and its Implications,* (University of Chicago, Chicago 1972); Louis Dumont, *Essays on Individualism: Modern Ideology in Anthropological Perspective* (University of Chicago Press, Chicago 1986)

[1416] Karl Marx, "On the Jewish Question 1844," in D McLellan (ed), *Karl Marx: Selected Writings* (OUP, Oxford 2000), 46-70; For similar perspectives, see C Taylor, *Philosophy and the Human Sciences: Philosophical Papers 2* (CUP, Cambridge 1985); M Walzer, *Spheres of Justice* (Perseus, NY 1984); A MacIntyre, *Against the Self-Images of the Age* (University of Notre Dame Press, Notre Dame 1978)

[1417] eg, as in Facebook, Bebo, LinkedIn, Friendster, hi5, Orkut.

7.3.1.3.3. Negligible stress on duties and responsibilities

De Hert's right to identity lays little stress on duties and responsibilities. It is not that De Hert makes no mention of duties, rather that when he does (in terms of State Parties undertaking to respect the right to identity), he fails to acknowledge that duties and responsibilities in respect of digital identity are not just limited to that high level. In this is further perpetuated what Bobbio called the "great turn of the West."[1418] But, what is more relevant and proposed by this thesis is an identity notion where the concept of duty is constitutive, and not merely accidental, to identity. Identity, in the collective sense, is also achieved by horizontal layers of duty relations that go beyond duties of state actors towards individuals to duties between individuals.

Duties and responsibilities are incumbent upon every person dealing with digital identity and every digital identity subject, not just the State. But the digital identity regulatory discourse, as with De Hert's proposal, has always explicitly and obviously focused more in terms of how rights must accrue or be given to individuals, with an eerie silence about duties.[1419]

This is challenging in two respects. First, digital identity problems can be attributed to duties in respect of digital identity not being respected. A certain right may exist in a digital identity, but unless and until a corresponding duty is performed in respect of it, that right has no meaning or significance. For instance, if a digital identity provider fails to perform its duty of providing me with a working digital identity, then though I may have a right to enjoy my digital identity; it is meaningless if it cannot be fulfilled.

[1418] Norberto Bobbio, *L'Età dei Diritti* (Einaudi, Torino 1990), 57. The "great turn of the west" occurred when rights as entitlements replaced duties in their primacy. For further discussion see Francesco Viola, 'Personal Identity in the Human Rights Perspective,' in A Peczenik, MM Karlsson (eds), *Law, Justice and the State I: Essays on Justice and Rights* (Franz Steiner Verlag, Stuttgart 1995), 100-109, 100

[1419] For India, particularly this is problematic given the extreme social and legal importance placed on duties. Raimundo Panikkar argues that the Hindu notion of *dharma* requires that human rights are not only the rights of individuals or even humans, and secondly that human rights involve duties and relate us to the whole cosmos. R Panikkar, 'Is the Notion of Human Rights a Western Concept? A Hindu/Jain/Buddhist Reflection,' (1982) 30 Diogenes, 75-102; Also Kana Mitra, 'Human Rights in Hinduism,'(1982) 19 J Ecu Studies 77

Second, the right to identity because it does not make significant expression of duties might find itself being questioned for relevance by legal collectivist cultures like India that demonstrate a higher regard for duties and responsibilities.[1420] While the right to identity might find deep resonance in legal cultures familiar with rights being bold statements of entitlement, other legal cultures would view this approach less favourably.[1421] They may thus not find much basis for taking it on since duties tend to be ranked at higher levels than entitlements[1422] and are viewed as highly contingent upon one another.[1423]

7.3.1.3.4. Postpones discussion of the remedial

While the right to identity intends to remedy harm resulting from the abuse of digital identity, the remedial element is not explicitly outlined. How is the right to identity expected to work in terms of providing an effective remedy in the case that its violation is found?

Even Article 8 of the UNCRC (right to identity) includes an explicit remedial element. Article 8(2) provides that, "Where a child is illegally deprived of some or all of the elements of his or her identity, States Parties shall provide appropriate assistance and protection, with a view to speedily re-establishing his or her identity."

In particular, a decision needs to be made if De Hert's right to identity is seen as a traditional human right that is efficient mainly against the state or the state actors, or as something that has direct effects against private parties such as ISPs. The argument developed in the previous chapters aims to recast the right to identity, away

[1420] HC Triandis, *Individualism and Collectivism* (Westview Press, Boulder 1995); DA Cai and EL Fink, 'Conflict Style Differences Between Individualists and Collectivists,' (2002) 69 (1) Communication Monographs, 67–87

[1421] Bas Rozemuller, 'Chinese Assumed Collectivism Revisited: A Study of the Labor Situation in a Sino-Western Joint Venture,' in Heidi Dahles and Harry Wels (eds), *Culture, Organization and Management in East Asia: Doing Business in China* (Nova Science Publishers, NY 2003), 39-84, 50

[1422] See Robert Kreitner, *Management* (HMH Publishing, Boston 2006), 103

[1423] See SH Nasr, 'The Concept and Reality of Freedom in Islam and Islamic Civilization,' in AS Rosenbaum (ed) *The Philosophy of Human Rights* (Greenwood Press, Connecticut 1980), 95-101, 95, 97; Douglas Hodgson, *Individual Duty Within a Human Rights Discourse* (Ashgate, Aldershot 2003), 25-26; John Carman, 'Duties and Rights in Hindu Society,' in LS Rouner (ed) *Human Rights and the World's Religions* (University of Notre Dame Press, Notre Dame 1988), 113-128

from a defensive right available against the State only, to a constitutive right against everyone, including oneself (the duty aspect again). In this respect too, it is a 'collective' right with similarities to third generation rights, important for countries with local conditions similar to India.

7.3.1.3.5. Uncertain future

It remains, however, to be seen whether the right to identity would have the effect desired. Going by the success of Article 8 UNCRC in protecting the right to identity, the prognosis isn't good. In the only case reported, Article 8 of the UNCRC was refused to be drawn upon in consideration of a child's right to privacy from media photography, in *Hosking and Hosking v Runting and Pacific Magazines NZ Ltd*[1424] The Court held that "the preservation of identity (Art 8).." was "directed at serious physical and mental abuse of children in situations," unlike this one. Will De Hert's right to identity have a similar fate? It is highly probable, if implemented in current form.

7.3.1.3.6. Application hurdles

The application of the right to identity has not been explored in great detail be De Hert. Where will this right fit? How will it be made to work to protect the rights of digital identity subjects? De Hert's approach is to some extent silent on these issues, reflecting an approach influenced by the experience of people in the west, where the presence of efficient administrative and judicial systems 'can take care of' these issues further down the line.

7.3.1.3.7. Primarily, a legal solution

Though envisaging the right to identity as a specific legal right, De Hert suggested it could be incorporated in the UNESCO's Code of Ethics for the Information

[1424](2005) 1NZLR 1. For commentary and case details see Katrine Evans, 'Hosking v Runting: Balancing Rights in a Privacy Tort,' [2004] PLPR 28; Katrine Evans, 'Reverse Gear for NZ's Privacy Tort: The Hosking Decision,' [2003] PLPR 35

Society.[1425] But, all in all, De Hert's right to identity, remains for the moment limited to a purely legal solution. But, the nature of digital identity makes it highly unlikely that a legal solution might be the optimal or most effective solution in all cases. The right to identity might be more effective in some cases and less effective in others, especially in societies like India where the law and local conditions conflict and "there is no widespread positive phenomenon of obedience to law which is simply enacted or judicially stated."[1426] In these situations, creation of secondary or 'grey' adjudication methods – a form of regulation by architecture – may after all be necessary to supplement legal solutions (here, identity management systems discussed in Chapter 4 come to their real strength and prevent a vacuum on regulatory protection).

7.4. Conclusion

The examination of the national legal solutions, particularly the Costa Rican right to virtual personality, Blackman's right to digital identity and Sullivan's right to database identity, show that they are rather limited. Most significantly, they make assumptions about the universal homogeneity of the digital identity subject and its ability to control digital identity. These solutions reflect principles that do not have global acceptability.

De Hert's right to identity is the most promising. Yet, it has several issues: the problem of the *ipse-idem* terminology, an individualist orientation, little stress on duties and responsibilities, insufficient emphasis on remedies and application hurdles. If these can be worked with, the right to identity might be a stepping stone to the next level of identity regulation taking into account the global and local contexts of digital identity. This is the challenge broadly taken up in the next chapter.

[1425] UNESCO, 'Code of Ethics for the Information Society,' (2007) <http://portal.unesco.org/ci/en/files/24935/11841676611Code_of_Ethics.pdf/Code%2Bof%2BEthics.pdf>

[1426] Cruz (1999) **n281**, 297, 298

8. The regulatory future of digital identity: The tri-elemental framework

> The tools are now within reach to permit sovereigns with competing rulesets to play down their differences whether by countenancing global privatization of some Internet governance issues, coming to new international agreements on substance and procedure to reduce the friction caused by transborder data flows, or by a "live and let live" set of localization technologies to shape the Internet to suit the respective societies it touches.
> -*Jonathan Zittrain*[1427]

8.1. Introduction

The legal proposals examined in Chapter 7 fall short of presenting a suitable digital identity regulatory solution for countries like India that, though subject to international influences in digital identity regulation, are conditioned by local difference. This chapter aims to remedy this situation. Acknowledging the inevitability of the influence of international legal trends, respecting the positive elements of De Hert's proposal for a right to identity and recognising the need to account for local difference, this chapter proposes a tri-elemental regulatory framework (TeF) for digital identity, based on the concept of *dharma.*

This framework is particularly addressed at India; the previous chapters (3, 5 and 6) reveal there is a pressing need for a terminology in relation to digital identity regulatory policy that will provide it legitimacy in the light of both global implementation and local difference. This is of particular importance given that digital identity regulation in India, as demonstrated in Chapters 5 and 6 is in disjoint with local realities.[1428]

8.2. *Dharma*

Dharma[1429] is an innate part of Indian philosophy, and particularly Hinduism (of which it is a fundamental concept). *Dharma,* as old as time and religion itself, is embodied with multiple layers of meaning. Its earliest expression is found in the

---

[1427] Zittrain (2003) **n43**

[1428] See Mary Hiscock, 'Changing Patterns of Regional Law Making in Asia,' (1995) 5, Australian Journal of Corporate Law, 367–933

[1429] The term *dharma* is of Sanskrit origin and derives from the root *dhr* which means to sustain, maintain or support. For more detailed analysis of *dharma,* see Robert Lingat, *The Classical Law of India* (University Presses of California, Columbia and Princeton, 1973)

dharmasutras, the ancient Indian authoritative treatises on it.[1430] In Hinduism, *dharma* represents,

> ideals and purposes, influences and institutions that shape the character of man both as an individual and as a member of society. It is the law of right living, the observance of which secures the double object of happiness on earth and salvation.[1431] For the perfect men, the dharma is an inspiration from within; for others it is an external command, what custom and public opinion demand.[1432]

But *dharma* is not just a religious concept; it is also a secular concept.[1433] It has legal significance;[1434] evident in the conceptualisation of *dharma* as a "comprehensive normative system which seeks to regulate the conduct of man towards all other beings and existences so as to preserve and uphold the Universe."[1435]

At this point, it must be clarified, as expressed before, that the choice of *dharma* is not an advocation of Hinduism being the 'right religion' or because its notions are ethically superior to other religions. Rather, the position taken here is a neutral, sociological one. The principles of *dharma* elaborated below are cultural concepts common across communities in India and intuitively function as an effective communication means to explain certain ideas to people. These are used to inform the digital identity regulatory discourse and revitalise it, particularly given the analysis of the preceding chapters (ie, 3, 5 and 6).

Dharma can be split into three categories: the right conduct (*Sad Achara)*,[1436] procedure for the enforcement of the right conduct (*Vyavahāra*) and rituals to make a person spiritually, culturally and socially pure (*Prayaschitta).*[1437] This categorisation

---

[1430] The most important are *Apastamba, Baudhayana*, *Gautama* and *Vasistha.* See Patrick Olivelle, *The Dharmasutras: The Law Codes of Ancient India* (OUP, Oxford 2009), xxvi
[1431] S Radhakrishnan, 'The Hindu Dharma,' (1922) 33 (1) Intl J Ethics, 1-22, 1-2. Citing *Abhyudaya* and *Nihgreyasa.*
[1432] Ibid, 4
[1433] SC Banerjee, *A Brief History of Dharmasastra* (Abhinav Publications, India 1999), 1
[1434] Per CM Lodha, J in *Gagan Raj Singh Nagori v Union of India* 1979 WLN 634; Justice M Rama Jois*, Legal and Constitutional History of India Vol I* (Universal Law Publishing, India 1984), 1-4
[1435] AD Mathur, *Medieval Hindu Law: Historical Evolution and Enlightened Rebellion* (OUP, Oxford 2007), xvii. *Dharma* is also called the Upanashadic concept of law. See also *Shri ASN Deekshitulu v State of Andhra Pradesh* 1996 AIR 1765 (SC)
[1436] Or ideal behaviour; sometimes transliterated as *Sad-ācāra.*
[1437] Mathur (2007) **n1435,** 224

is derived from Sage *Yājñavalkya*'s categorisation of *dharmashastra*[1438] into *Achara* (ritual), *Vyavahāra* (jurisprudence) and *Prayaschitta* (reparation), elaborated in the *Yājñavalkya Smriti*.[1439] These three categories offer considerable insights into how digital identity problems could and might be dealt with and have much to contribute to the legal regulatory future of digital identity.

8.2.1. *Sad Achara:* The right conduct

Sad means good or righteous and *Achara* means conduct. Aligned together, *Sad Achara* means righteous behaviour or conduct. It is doing the right thing according to prescribed or acceptable standards of conduct. The *Hari-bhakti Vilasa* states that "he who does not maintain the standards of conduct is neither noble nor righteous."[1440] Thus, a person's adherence or non-adherence to *Sad Achara* determines their character. If a person's conduct is characterised as *Sad Achara*, that person is holy, noble and virtuous. *Dur Achara*, or bad or deviant conduct, is the reverse of *Sad Achara*. *Sad Achara* traditionally manifests in the performance of daily rituals,[1441] sacraments[1442] and living life according to the *Ashramas.*[1443] In all that it represents, *Sad Achara* basically entails engaging in the right, acceptable or prescribed conduct.

The ambitions of *Sad Achara* are reflected in the Ten Commandments in the Old Testament,[1444] which are prescriptions of right conduct for Jewish and Christian believers. In their enunciation, they represent ethical considerations for social life;[1445] "social and moral requirements" of conduct and what is "right and wrong in human

---

[1438] The science of *dharma.*
[1439] The *Yājñavalkya Smriti* is one of the most important *Smritis* (post Manu) comprising of approximately 1,010 verses and an important source of Hindu law. Also see M Nath Dutt, *Yajnavalkyasmrti: Sanskrit Text, English Translation, Notes, Introduction and Index of Verses*, (Parimal Publications, New Delhi 2005) and P Olivelle, 'Dharmaśāstra: A Literary History,' in T Lubin and D Davis (eds), *Cambridge Handbook of Law and Hinduism* (CUP, Cambridge 2010), 28-57
[1440] *Hari Bhakti Vilasa*, 3, 15-16
[1441] Daily rituals include *snana* (bathing), *japa* (prayer, citation of mantras), *homa* (sacrificial offerings) *devapuja* (worship of God), *aathithya* (hospitality) and *vaisvadev* (food offerings to God).
[1442] Sacraments consist of *upanayana* (sacred thread ceremony), *vivaha* (marriage) and *antyeshthi* (death ceremonies).
[1443] *Ashramas* comprise of four life stages: *brahmacharya* (instructive stage of life), *grihastha* (the householder stage of life), *vanaprastha* (withdrawal from life and retreat into the forest) and *sanyasa* (renunciation)
[1444] See Deuteronomy, *The Bible,* Ch 5, verses 6-21. PD Miller, *Deuteronomy* (John Knox Press: USA 1990), 71-96. The Islamic equivalent is the *Sunnah.*
[1445] W Barclay, *The Ten Commandments* (Westminster John Knox Press, Louisville 1998), 1

conduct."[1446] The same is reflected in *Sad Achara* and *Dur Achara.* Conduct in accordance with the Ten Commandments is *Sad Achara* and conduct contrary to the Ten Commandments is *Dur Achara*.

However, despite this similarity, there is an important difference. The conceptualisation of (religious) duties in the Judeo-Christian tradition is, as indicated, as *commands*. They are an obligation primarily towards a higher authority whose commands allow pre-established individuals (as God's creation) to interact with each other. In secular Western philosophy that partly replaced these religious terms, the "unencumbered self" that underpins the liberal vision of society predates legal order.[1447] This translates quite naturally into a picture where free individuals interact primarily with a higher level norm-giver, the State, that allocates rights and duties through the Constitution and also other primary legislation. It is this norm giver towards whom primarily a duty is owed, and who in turn, through law can be restricted in the exercise of power.

Sad Achara under *dharma* is subtly different. Here, the system of obligations is not externally imposed on previously free individuals, but *constitutes* individuals through a horizontal system of duties - duties towards others arising from and constituting what an individual truly is. Acting against duties diminishes an individual (by being driven by illusions or *Maya* and thus giving that individual false ideas of what it truly is[1448]) as much as it harms others. The difference is subtle, and allows the Indian approach too to be roughly approximated by and where necessary translated into the (western) language of legal rights. However, in some contexts this will result in equally subtle differences in legal outcomes and emphasis. But it is an approximation only, and law, in this picture becomes a "theology of everyday life"[1449] revolving around the household, family and everyday relationships – the state with its institutions and norms is, unlike in the West, not constitutive for these rights and duties, but merely facilitative.

[1446] JP Hester, *The Ten Commandments: A Handbook of Religious, Social and Legal Issues* (McFarland and Co, North Carolina 2003), 27
[1447] See in particular Michael J Sandel, 'The Procedural Republic and the Unencumbered Self,' (Feb 1984) 12 (1), Political Theory, 81-96
[1448] TVG Sastri, 'General Concept of *Maya* and its Applications,' (1975) 24, J Oriental Inst 343-356
[1449] Davis (2010) **n78**, 1

Digital identity problems can be attributed to a lack or disregard of *Sad Achara.* The unauthorised use or sharing of digital identity, the discriminatory use of digital identity, denial of access to digital identity, erasure or obliteration of digital identity and digital identity fraud are all examples of *Dur Achara*. It is because persons behave in these discriminatory and unauthorised manners that digital identity problems arise.

Sad Achara would therefore necessitate a duty in respect of digital identity.[1450] Here are some examples. Digital identity subjects have a duty to use their digital identities appropriately (generally prescribed in the ToS or EULAs). Digital identity providers may incur a duty to ensure that digital identity subjects have accessible use of their digital identities and that digital identities are kept secure, up to date and accurate. States might be obliged to foster conditions favourable to the enjoyment of digital identity and in the case of digital identity breaches or compromises, to provide adequate redressal mechanisms.

This duty based element of digital identity, while not entirely ignored, has been an underused element in digital identity regulation (see Chapter 7). When duty has been a matter of focus, it has been emphasised very broadly and fairly insignificantly. This can be attributed in large part to the overt focus, in the digitally advanced West, on 'rights' of the digital identity subject. Compounding this, is how duties are shrouded in terms of obligations owed by other stakeholders (like businesses, governments and other organisations) to the individual digital identity subject, as explained in the diagram below:

[1450] The duty element of the proposed right finds substantial grounding in the Indian legal system, both ancient and contemporary. Duties had a supremely important place in ancient and medieval India and retain their significance in contemporary India. See SP Sharma, *Indian Legal System* (KMR Mittal, Delhi 1991), 21, Justice ES Venkataramiah, *Citizenship, Rights and Duties* (BV Naga Publishers, Bangalore 1988).There has been some movement in the West re-acknowledging the role of duties. See David Selbourne, *The Principle of Duty: An Essay on the Foundations of the Civic Order* (University of Notre Dame Press, 1997); Catherine Haire & Michael Manley-Casimir, 'Restoring 'Duty' to the Discourse of Rights and Citizenship Education: A Radical Retrenchment?' Paper presented at the XXVII Annual Meeting of the Canadian Society for the Study of Education, University of Sherbrooke (Quebec, 1999)

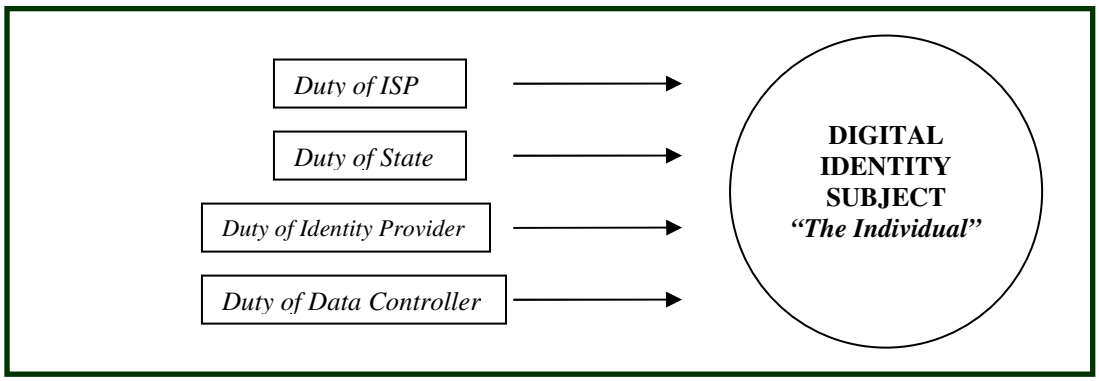

Fig 8: Duties as Visualised in Previously Proposed Legal Solutions

But, in respect of digital identity, *Sad Achara* is a much more versatile concept that encompasses duties on the part of all stakeholders in relation to digital identity - whether it is individuals, private entities, organisations or States.

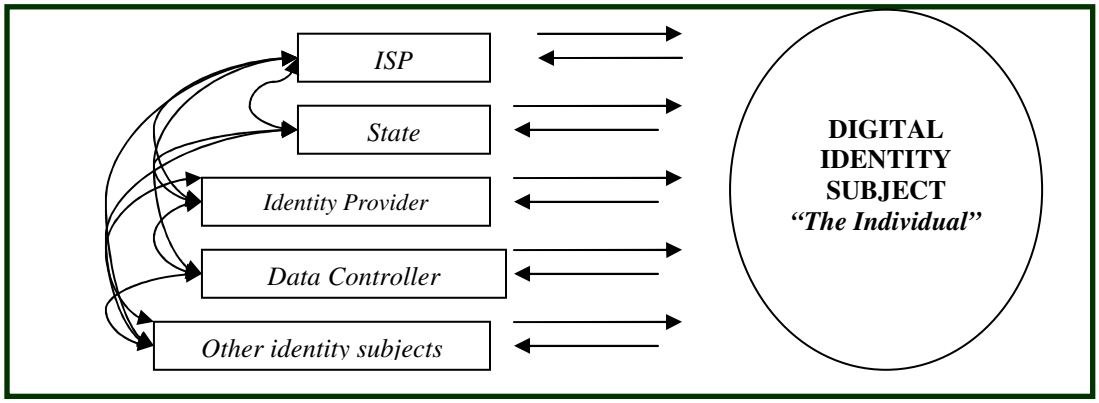

Fig 9: Duties per *Sad Achara* and the TeF

Every digital identity stakeholder has a duty to another digital identity stakeholder. On this basis,

It is every person's duty to respect the digital identity of another

8.2.2. *Vyavahāra:* Procedure for enforcement of the right conduct

Vyavahāra was a very important source of ancient Hindu law.[1451] It is mentioned several times in Indian philosophical literature like the *Smritis* and commentaries in a

[1451] DD Aggarwal, *Jurisprudence in India Through the Ages* (Kalpaz Publications, New Delhi 2002), 59

number of senses - as civil law, positive law and legal procedure.[1452] Kane's definition puts *Vyavahāra* into perspective*:*

> When the ramifications of right conduct, that are together called *dharma* and that can be established with efforts (of various kinds such as truthful speech, etc.) have been violated, the dispute (in a court between parties) which springs from what is sought to be proved (such as debt), is said to be *vyavahāra.*[1453]

Sad Achara might not always be maintained in respect of digital identity and digital identity conflicts might arise. Then, *Vyavahāra* becomes important.

Vyavahāra in relation to digital identity supports a procedural framework for the resolution of disputes. If digital identity is to be protected and the right conduct is to be supported in its existence, application, and enjoyment, then there must be a framework (whether legal, technical or policy based) to enable this.
A digital identity subject must be able to experience digital identity to the best and fullest extent possible.[1454] But this experience is subject to legal, policy, social and technical factors; one, some or all of which might work to promote this end, undermine or limit it. It might not always be the case that a duty in respect of digital identity is able to be fulfilled. This is another context in which procedure becomes very important.

While policy, social and technical procedures are important in resolving and alleviating digital identity disputes, law (and legal procedure) must function as the definitive safeguard of digital identity. Law must establish or prescribe conditions for the enjoyment or curtailment of digital identity. It must set forth, determine and apply not just the conditions for the enjoyment of digital identity, but also specifically outline the circumstances under which digital identity might be curtailed or legitimately interfered with.[1455]

Vyavahāra thus necessitates that:

[1452] Aggarwal (2002) **n1451,** 58
[1453] PV Kane, *History of Dharmaśāstra*, Vol. 3, (BORI, Pune 1946), 247
[1454] This is one of the aims and purposes of identity management technology and law.
[1455] There will always be occasion for these kinds of situations to arise; however controversial this might be, there can never be an absolute right to digital identity.

No person shall be deprived of digital identity except according to procedure established [prescribed][1456] by law

While this statement seems innocent enough, it encapsulates the most radical (and arguably most controversial) aspect of the recasting of the right to identity from an individual right to a bundle of duties. First, it creates a burden on the state vis-a-vis the citizen. Where the government, under the agenda of economic progress or for reasons of security, creates channels of communication with its citizens that require a digital identity (from e-government initiatives to biometric passports), it creates a burden to provide for the efficient and substantial, not just formal, opportunity for all citizens to engage with the State in this way. At the very least, this creates a substantial and enforceable 'due process' burden when for instance an application for a biometric passport is rejected or a digital identity subject is refused access to a government run digital platform.

As with the death penalty, mere technical or minor violations of duties by the citizen will not normally be sufficient to warrant termination of an identity, especially when under the socio-economic realities, the citizen had little choice but to technically violate one of these rules (e.g., registers for a government service with a "borrowed" ID from a shared email account, or if in the rural community the only access to the net is through such informally shared facilities).[1457] It also creates a burden on the state to provide an appropriate infrastructure, which could entail free email or online accounts for citizens otherwise excluded from such services – in line for example with the legal requirement, discussed in the UK, to provide minimum banking facilities and accounts for poor citizens through the post office, or as a legal duty on ISPs. It is acknowledged though that this type of "economic right" as with all third generation rights, poses unique difficulties for actual enforcement.

While this type of duty on the state is closest to the way in which de Hert and others discuss a right to identity,[1458] our framework of a system of vertical and horizontal duties does not stop here. The duty also encompasses horizontally the relation

[1456] Some jurisdictions like the UK show preference for this term.
[1457] See **Ch 6 (6.3.2),** case study on Sharing.
[1458] See **Ch 7**

between the digital identity provider, e.g. an ISP and the user. At the every least, it requires transparent and fair due process procedures before a digital identity is terminated. In addition, as above, not every technical violation of contractual terms will normally permit such a termination, even though the demands will be lower than in the case of state action, expressing the importance of the reciprocal duties or *Sad Achara* of the user towards the identity provider.

Unlike the Western model with its emphasis on individual autonomy, this protective regime cannot always be waived through contractual agreement. Not any more than in the offline world can the arbitrary termination or violation of digital identity be consented to. This paternalistic approach, which in the context of Western law corresponds to a very strong 'good faith' interpretation of contractual terms, reflects again the different socio-economic realities. There are power differentials between identity providers and users, both in terms of the economic ability to defend themselves against unfair termination or find feasible alternative providers, and in terms of their education and understanding of the legal implications of the contract.

Finally, the protection of identity also accrues to an individual against other individuals. We have mentioned several times the social practice of sharing digital identities, e.g. through joint use of scare resources like mobile phones.[1459] *Vyavahāra* in this case can also create duties on the lender which the law ought to recognize, at least in parts. This can entail a requirement to give 'fair warning' when such a facility is withdrawn, grace periods and other help to permit the person affected to migrate his established digital identity to another system etc. The closest Western translation of this idea is the concept of reliance liability when a reasonable expectation of continuous use was created on which a person relied. In this case, it would operate within a 'gift relation', an idea that may be more acceptable to lawyers from civilian jurisdictions who think of gifts as contracts that can also create duties on the donor, but may be more difficult to communicate to lawyers from the common law tradition where contracts require consideration to impose reciprocal duties.

[1459] **Ch 3 (3.2.1.4)**

8.2.3. *Prayaschitta:* Reparation

Prayaschitta is the third essential aspect of *dharma*. The *Bhagwadgita* alludes to the importance of *prayaschitta* in Chapter 18(5), which states that "Acts of sacrifice, charity and penance are not to be given up; they must be performed. Indeed, sacrifice, charity and penance purify even the great souls."[1460] *Prayaschitta* means atonement, reparation or expiation for sin *(pap*) and includes any measures taken to make a person pure. A person who commits any form of wrongdoing must make amends in respect of that wrongdoing. *Prayaschitta* removes and alleviates the effects of the wrongdoing. *Prayaschitta* has two elements: *prayas* meaning penance and *chitta* meaning knowledge. Thus *prayaschitta* means "penance performed with the knowledge of wiping off sin."[1461] The *Dharmashastras* visualise various categories of sin or wrongdoing and different expiatory rites to deal with these.[1462] They also acknowledge that mitigating circumstances may affect the nature of the penance.

The concept of *Prayaschitta* has legal significance. This is supported by two factors: first, its inclusion as an element of law in the ancient Hindu legal texts and second, its use and citation in Indian case law. *Prayaschitta* features as a crucial element of law in a number of ancient India legal texts like the *Manu Smriti*[1463] and the *Mitakhsara*[1464] (*Prayaschitta Adhayaya*). *Prayaschitta* has been referred to in Indian legal cases like *Parami Ramayya v Mahadevi Shankarappa,*[1465] *Govind Das v Bishambhar Das,*[1466] *Vaman Deshpande v Krishnaji Kulkarni*,[1467] *Bai Gulab v Jivanlal Harilal,*[1468] *Bhikubai Meher v Hariba Meher,*[1469] *SK Wodeyar v Ganapati*

[1460] Available online at <http://www.bhagavad-gita.us>
[1461] SC Banerji, *A Brief History of Dharmasastra* (Abhinav Publications, Delhi 1999), 90
[1462] DC Bhattacharya, 'Penances and Vows,' in CPR Aiyar (ed), *Itihasas, Puranas, Dharma and Other Sastras: The Cultural Heritage of India Vol II,* (RMIC, Calcutta 2003), 381-389
[1463] The most ancient and authoritative Hindu *smriti*. Here, *prayaschitta* echoes incessantly as a means of making amends and source of purification.
[1464] An influential Hindu legal treatise by Vijñāneśvara which is largely a commentary on the *Yājñavalkya Smriti.*
[1465] (1910) 12 BOMLR 196
[1466] (1917) ILR 39 All 561
[1467] (1919) 21 BOMLR 427
[1468] (1922) 24 BOMLR 5
[1469] (1925) 27 BOMLR 13

Dixit,[1470] *Goona Durgaprasada Rao v Goona Sudarsanaswami,*[1471] *Gagan Raj Singh Nagori v Union of India*[1472] and *Maruti Shripati Dubal v State of Maharashtra.*[1473]

In respect of digital identity, *prayaschitta* contributes two things. First, it links the abstract duties described above to a system of remedies similar to the remedies available under contract and tort (delict) law. When there is a duty (legal or otherwise) to respect a digital identity and that duty is not performed or is breached, the person responsible for discharging that duty must make suitable amends to the person who has been harmed as a result of the non-performance or breach of that duty. Let's take an illustration. Personal data is stolen from the National Identity Database and used to the disadvantage of the data subjects causing them financial and emotional harm. It is found that there was an internal breach in the maintenance of the security of the National Identity Database. The organisation in charge of maintaining the database security is found to be negligent. It thus has to make good the harm caused to the data subjects. This is *prayaschitta.*

Thus, *prayaschitta* necessitates that a digital identity subject deprived of its digital identity must be restored to the use of that digital identity, where possible. If restoration is frustrated, then other compensatory measures must be taken. Whoever is responsible for depriving the digital identity subject of their digital identity shall be liable to make amends in respect of that digital identity.

So far, the approach stays within the well known conceptual territory of contract and tort law. It ensures that a right to digital identity is not an abstraction, but has real and tangible consequences. As seen in chapters 2 and 3, digital identity is a multifaceted phenomenon. Furthermore, the ignorance of the legal regulatory framework is one of the main reasons why the protection of digital identity and related rights such as privacy in real life, as opposed to abstract legal protection 'in books,' often lacks on the ground.

[1470] (1935) 37 BOMLR 584
[1471] (1940) 1 MLJ 800 (Chennai)
[1472] 1979 WLN 634
[1473] 1987 (1) BomCR 499

A legal approach that is equally fragmented and creates new statutory remedies for each of the often very technical and technology specific expressions of digital identity, or laboriously derives them through analogous application of common law cases, would exacerbate this problem. Legislating for a population where access to digital resources remains a challenge makes this prohibitive. Instead, *prayaschitta* functions here similarly to the general clause of delict law in the German Civil Code that creates a bundle of non-specific remedies under the catch all provision of a violation of 'every other right' in Article 823.[1474] Similarly here, *prayaschitta* would make any violation of someone's digital identity directly actionable, independent of the specific nature of the digital identity in question, or how or by whom it was violated. This uniform approach ensures that once an individual understands the relevant reciprocal duties in the first and second elements of the TeF, an understanding that there is also a remedy available follows immediately. By ensuring that the framework itself is firmly rooted in culturally mediated understandings of digital identity, knowledge of available remedies becomes a non-issue.

Potentially though, *prayaschitta* can go further than this idea of direct actionable protection against violations of digital identity. So far, the general framework is still beholden to the Western concept of adversarial litigation that pits one right holder against the other. If my right to digital identity is violated by another person, I can sue him for appropriate relief. This adversarial approach that reduces a conflict to a private issue between two actors only is maybe the most important organising principle of Western private law - what Weinrib calls the bi-polar nature of the concept of private law.[1475] It excludes systematically the interests of the wider community from disputes between private parties, negates the values of distributive justice and requires an aggressive attitude towards the infringer of rights.

[1474] See BS Markesinis, Hannes Unberath, *The German Law of Torts: A Comparative Treatise* (Hart, Oregan 2000), ch 2; Also PR Handford, 'Moral Damage in Germany,' (1978) 27, ICLQ, 849-875. For the relation to privacy see B Markesinis, 'Privacy, Freedom of Expression and the Horizontal Effect of the Human Rights Bill: Lessons From Germany,Wilberforce Lecture 1998, (1999) 115 LQR, 45-88, 47

[1475] Ernest J Weinrib, *The Idea of Private Law* (HUP, 1995), 22

It is well known that the litigatious culture that this approach fosters is of limited suitability for Asian countries, where the communal approach means that even if a party wins in this kind of conflict, loss of face and social stigma may outweigh any financial compensation. As a result, the under-enforcement of rights is a persistent feature of Asian cultures that transplanted a Western approach to private law.[1476]

At the same time, aggressive enforcement of rights by powerful legal entities such as ISP's against users, even if they are remiss in their duties, can create disproportionate hardship (and bad publicity for the ISP). The concept of *prayaschitta* may have the potential to address this deficit to a degree. In addition of its translation and role as 'remedy,' it also carries the connotation of 'penance'. It is not something done necessarily exclusively to the benefit of the wronged party, it is also a public act of 'cleansing one's soul' by appropriate actions of contrition. These may also benefit parties other than those directly wronged, for instance through public giving to charity. While this notion can't be developed in full here, its conceptual potential should nonetheless be noted.

It may well be the case that the law should take cognisance of relevant and appropriate acts of 'penance' performed by a perpetrator before litigation even commences, even where the beneficiary is someone else than the person wronged. Such acts of contrition were, in traditional Hindu law, considered as a mitigating factor when the King imposed punishment for wrongdoing,[1477] and in the same way could be considered as a mitigating factor in civil litigation - or as a form of punitive damage even, that goes beyond restoration of the status quo. This possible Janus face of *prayaschitta* is particularly suitable for a society with huge economic and digital inequalities.

[1476]See eg, Marc Galanter, 'India's Tort Deficit: Sketch for a Historical Portrait,' in DM Engel, MW McCann (eds), *In Fault Lines: Tort law as Cultural Practice* (SUP, Stanford 2009), 47-65; Ananyo Basu, 'Torts in India: Dharmic Resignation, Colonial Subjugation, or "Underdevelopment"?' The South Atlantic Quarterly, (Fall 2001), 100 (4), 1053-1070. For other Asian cultures see eg, VH Li, *Law without Lawyers: A Comparative View of Law in China and the United States* (Westview, 1978)

[1477] PV Kane, *History of Dharmasastra: Ancient and Medieval Religious and Civil Law in India Vol 4* (BORI, Pune 1962-1975). This is the most comprehensive and authoritative treatise on the concept. For the specific issue and the relation between penance and state sanction see Vol 4, 12

In this way, the violation of duty by an impoverished individual (think again of unlicensed sharing) may be appropriately remedied by an act of penance towards a third party (e.g., an charity nominated by the ISP), while a violation of a user's right to identity by a powerful and rich corporation may attract in addition to the remedial element of *prayaschitta,* a punitive 'malus' for the benefit of the wider community. In both cases, litigation ceases being a conflict between two private parties locked adversely and becomes a process of wider social healing. Not by coincidence, this notion aligns with more recent attempts in the West to offer alternative forms of dispute resolution that are based on a notion of restorative rather than punitive sanctions.[1478]

In this light,

> **Appropriate and effective remedies shall be available to all digital identity stakeholders affected by actions against digital identity.**

Therefore, a TeF for digital identity (comprising of three elements of *right conduct, procedure for enforcement of the right conduct* and *remedy*) is proposed to guide and constructively encourage the future regulation of digital identity.

This TeF reiterates the importance of identity, because, contrary to Gutwirth's comments about identity being an absurdity,[1479] its importance cannot be dismissed, particularly given technological identity centricism and dependence; even though identity may not have all the solutions to the problems of the technological age.

But it is worthwhile to ask how the elements of the TeF relate to the existing Indian legal framework.

The first element, the duty, finds excellent grounding in the Indian legal system, both ancient and contemporary, and particularly in the Indian Constitution. The Indian

[1478] Cao Pei, 'The Origins of Mediation in Traditional China,' (1999) 54 Disp Res J, 32
[1479] **n1402**

Constitution incorporates a chapter[1480] on duties for citizens called Fundamental Duties, which though not justiciable like fundamental rights, have equal importance[1481] and obligate people to "develop a scientific temper and humanism," and "strive towards excellence in all spheres of individual and collective activity so that the nation constantly rises to higher levels of endeavour and achievements."[1482]

Even though the section on fundamental duties was only inserted into the Constitution in 1976, the debates of the Constituent Assembly in 1949 addressed the nature of the relationship between rights and duties in the Indian context: that every right implied and included a duty, that these went hand in hand and were two sides of the same coin - the obverse and the reverse.[1483] The importance of duties was further reiterated in landmark cases like *MC Mehta v Union of India & Others*,[1484] *Union of India v Naveen Jindal & Anr*,[1485] *Dr. PR Ramanujam v Indira Gandhi National Open University*[1486] and *Rameshkumar Sumersingh Barolia v Commandant*.[1487]

The second element of the framework, is a negative obligation, that no person shall be deprived of digital identity except according to procedure established (or prescribed) by law mirrors the text of Article 21 of the Indian Constitution (protection of life and personal liberty), on the right to life, which of all the rights is the most basic and deep seated and dynamic. It states that no person shall be

[1480] Chapter IV-A, Art 51-A (a-j) inserted into the Constitution by the Constitution (Forty-Second) Amendment Act 1976, s 11 (w.e.f 03/01/1977); and (k) inserted by the Constitution (Eighty sixth) Amendment Act 2002, s 4
[1481] Justice ES Venkataramiah, 'Citizenship Rights and Duties,' CILQ, (18 August 2009), <http://indiankanoon.org/cached/1796518/>
[1482] *AIIMS Students' Union v AIMS*, SC CA 7366 of 1996
[1483] Constituent Assembly Debate on the Government of India Act (Amendment) Bill, 25 November, 1949. See <http://indiankanoon.org/doc/1473869/>
[1484] 1988 AIR 1115
[1485] SC CA 2920 of 1996 (every right is coupled with a duty)
[1486] Delhi High Court, Judgment of 25/9/2006, <http://indiankanoon.org/doc/355555/>
[1487] Gujarat High Court, SRP, 10 February 1999 <http://indiankanoon.org/doc/1566221/. Duties and rights are "two facets of the same coin."

deprived[1488] of his life or personal liberty except according to procedure established by law.[1489]

The third element, appropriate and effective remedy, is a basic element of law (constitutional or otherwise). Remedies for violation of fundamental rights are enshrined in Articles 32 and 226 (writ issuing powers) of the Indian Constitution.

Thus, the elements of the TeF have good basis under core Indian law.

Next, one must note the paradox presented before us – in terms of the high standards suggested here and those characteristic of the Indian system described in Chapters 5 and 6. The law regulating digital identity in India is particularly influenced in its spirit and letter by external norms due to its borrowed nature. Though it overtly seems to regulate digital identity in theory, in practice there are also adverse effects, such that the Indian digital identity subject is at a disadvantage as compared to its Western (particularly European) counterpart. The high standards,[1490] presented here in the TeF, are a reminder and call to the Indian State (the legislature, judiciary and executive) to re-work and adapt its regulatory perspective more holistically taking into account the local conditions of digital identity subjects and simultaneously the global nature of digital identity.

8.3. Evaluation of the TeF

The TeF represents a significant step forward for the regulatory future of digital identity. However, this attempt (at presenting a solution inspired by Indian religion and law) does not in any manner claim the ethical or religious superiority of a particular religion or jurisdiction over others; it simply uses a concept that is

---

[1488] For the scope and an illustration of what constitutes deprivation see: *Francis Coralie Mullin v The Administrator, Union Territory of Delhi & Ors; Olga Tellis & Ors v Bombay Municipal Corporation* 1986 AIR 180, 1985 SCR Supl. (2) 51; *Maneka Gandhi* **n734**

[1489] 'Procedure established by law' was adopted from Article 31 of the Japanese Constitution. For intrepretation see *AK Gopalan v The State of Madras* 1950 SCR 88; Maneka Gandhi **n734**; *MH Hoskot v State of Maharashtra* AIR 1978 SC 1548; *Francis Coralie Mullin v the Administrator, UT of Delhi and others* [1981] 2 SCR 516; *Olga Tellis* **n1488**

[1490] These high standards are in accord with the life and culture of the Indian digital identity subject as revealed in Chs 3, 5 and 6, particularly the norms that reveal that the individual is not considered as compared to the West, the 'final end of existence.'

instantaneously intelligible across Indian (given its internal cultural fragmentation) and other international communities to advance the future regulation of digital identity.

This section outlines the value added the TeF brings to the regulation of digital identity.

8.3.1. Participatory

The previous rights based solutions[1491] proposed for regulating digital identity fell short in respect of the participatory element. The solutions did not adequately or equally involve the digital identity stakeholders in terms of making them realise their contribution in performing their mutual duties. If all stakeholders are made aware of this and act upon this then they would become more drawn into the process of the regulation of digital identity. This is what the TeF seeks to promote. It acknowledges the positive and active role of all digital identity stakeholders and calls for their galvanising together, particularly through the first element – the duty of all persons towards each other in respect of digital identity.

8.3.2. Holistic

The TeF represents a complementary combination of elements in the regulatory context: duty, procedure and remedy. If a duty is evident, then there must be procedure to enforce it; if a violation is found, there must be an effective remedy. The combination of elements makes the framework highly relevant and applicatory.

For instance, an identity provider has a general duty to provide a digital identity subject with reasonable access to its digital identity. If the digital identity subject cannot access its digital identity, it must be able to complain to the identity provider and get the identity provider to take such actions as would restore access. If the digital identity subject cannot have access to its original identity, then alternative

[1491] Outlined in **Ch 7**

identity and access arrangements must be made by the identity provider. This solution is already evident in the manner how usernames and passwords work.

8.3.3. Balanced

Balance is one of the under-focussed elements in the digital identity discourse.[1492] The new TeF would achieve the delicate and controversial balancing of different digital identity stakeholder interests. It does not, like previous approaches, seek to place one digital identity stakeholder in priority over another. For instance, the TeF does not promote that an individual is entitled to absolute digital identity rights, as Sullivan does.[1493] In reality, there are very few absolute rights,[1494] all of which are only available to human persons. [1495] It is highly unlikely a right to identity would be accepted and achieve its full potential as an absolute right against which no limitations or derogations apply.[1496]

Any right to digital identity, unlike as presumed before, does not operate in isolation to social,[1497] technical[1498] and legal[1499] contexts. Digital identity stakeholders and subjects in particular, come from different social and legal jurisdictions. The TeF recognises this and aims to achieve the best balance in these settings.

8.3.4. Dynamic

The TeF, in addition to being legally relevant, is also of significance to the policy and technical aspects of digital identity. The framework could be used to guide digital identity policy. For example, in developing ToS and EULAs. These

---

[1492] Recognised by De Hert.
[1493] A highly utopian vision.
[1494] An absolute right is defined as a "right set out in the European Convention on Human Rights that cannot lawfully be interfered with, no matter how important the public interest in doing so might be," *Oxford Dictionary of Law* (OUP, Oxford 2009), 3. Absolute rights under the ECHR include: prohibition on torture (Art 3), prohibition on slavery and forced labour (Art 4) and right to fair trial (Art 6). It has been contended that there is no such thing as absolute rights, see discussion in Alan Gewirth, 'Are There Any Absolute Rights?' (1981) 31 (122) The Philosophical Quarterly, 1-16
[1495] But a digital identity subject is not always a human being. For instance, AI agents, robots, other non-human legal persons.
[1496] This is because digital identity is still evolving in its relationship with the person. There is also a difference, as seen in **Chs 2 & 3** of the importance of digital identity to the individual in different jurisdictions.
[1497] **Ch 3**
[1498] **Ch 4**
[1499] **Chs 5, 6 & 7**

agreements incorporate strong terms of conduct, prohibitions and procedure and consequences for non-compliance. They weigh heavily in favour of the drafter of the agreement (e.g. the identity service provider). These agreements could learn from the TeF. Agreements could be made more balanced (in terms of incorporating duties and rights for both parties as well as appropriate and effective remedies in the event that either party to the agreement violates the same.)

The framework could also be used as a technical principle like the Laws of Identity. Technologists could build systems grounded on the elements of the framework. Systems might thus aim to facilitate the right conduct (*Sad Achara*), ensure that all actions in respect of digital identity have legal basis (*Vyavahāra)* and if digital identity is harmed or affected, make available appropriate and effective remedies (*Prayaschitta).*

8.3.5. Evaluatory mechanism

The framework could be used a guide in implementing laws and regulations concerning digital identity, and to evaluate existing laws and regulations concerning digital identity. In this respect, the framework could function as a macro or micro level tool. At the macro level, it could help evaluate the overall efficacy of the law and at the micro level, individual provisions of legislation. If the law, at the macro or micro level is found to be deficient, then measures could be taken to increase efficiency. In similar manner, it could be used as a digital identity policy evaluatory tool or a technical evaluatory guide.

8.3.6. Universally relevant

One of the key challenges for the regulatory future of digital identity is to find a solution with universal appeal and simultaneous local relevance. Earlier in the thesis, it was evidenced that though digital identity and identity management are global phenomena,[1500] the legal regulation[1501] and local conditionality[1502] of digital identity are not.

[1500] **Chs 2 & 4**
[1501] **Chs 5 & 6**

The TeF is more globally relevant that any other solution. Its three elements are recognised, in some form or the other, in most legal systems of the world,[1503] albeit to different degrees depending on the contexts (which is not necessarily a debilitating, but rather positive feature). Though it finds inspiration in *dharma,* its elements find basis in most law and have universal significance.

Its departure from the accepted position of 'individual as the holder of a definite right,' the TeF (with a collective, collaborative dimension) is well suited to societies and legal cultures that do not subscribe to this principle,[1504] and yet which are key players in the regulatory future of digital identity. Each digital identity subject must perform their duty to respect digital identity, whatever the digital identity context. There is to be no denial of the right except through well established legal procedure and recourse to remedy in cases of digital identity abuses. This is something that has universal validity and concurrent local applicability.

8.3.7. Resource based solution

One of the key factors highlighted in Chapter 3 was local difference in terms of how the state of digital identity technologies between countries differed.[1505] This affects the experience and must be taken into account in the regulation of digital identity. The TeF in presenting itself thus, is versatile enough to be adopted either as a legal,[1506] technical or policy measure; whichever best suits local conditions and priorities.

[1502] **Ch 3**

[1503] English Common Law recognises duties, legal process and remedy. See Sir William Blackstone**,** *Commentaries on the Laws of England, Vol I* (Collins, NY 1832), 60, 88, 176, 394. Islamic law recognises the place of duty of the right conduct to God and man, adherence to prescribed religious tenets equal to law, and reparation in the form of punishment. See RM Savory, 'Law and Traditional Society,' in RM Savory (ed) *Introduction to Islamic Civilisation* (CUP, Cambridge 1976), 54

[1504] Note for example in India and particularly Hindu thought, that rights are not seen in terms of individual powers. See A Sharma, *Hinduism and Human Rights: A Conceptual Approach* (OUP, New Delhi 2004), 14, 19, 32, 34. Sharma states, "Hinduism tends to accord greater recognition to the rights others have in relation to us as compared to the rights we have in relation to them."

[1505] See **Ch 3 (3.2.1)**

[1506] The translation of the TeF into a legal right is a prospect for building on the work in this thesis, particularly in the Indian context.

8.3.8. Anchored in the *Volksgeist*

Perhaps the most important aspect of the TeF is its ability to accord with the *Volksgeist.*[1507] While representing itself a solution capable of universal application, in the Indian context, in its grounding in *dharma,* enables it to have cultural meaning and validity. Thus it aims to rectify the problems identified in Chapter 6, in according with the legal mentalité, and being directly a product of Indian people, their culture and daily lives. For the first time, Indian digital identity could be regulated through a locally matched solution that could lead to improved compliance and efficacy.

8.4. Conclusion

This chapter makes a significant contribution to the discourse on the regulation of digital identity, taking into account global implementation and local difference. The proposed holistic framework for the regulation of digital identity brings together a critical trinity of elements that represents a useful way forward for the future regulation of digital identity. As proposed, the framework is dynamic enough to fit the Indian[1508] and international contexts in different manners demonstrating its international acceptability and resilience.

[1507] See **Ch 1 (1.3)** and **Ch 6 (6.4)**

[1508] The thesis has identified in **Chs 5 & 6** a glaring gap particularly in terms of the explicit expression of the protection of a digital identity subject's rights in India, though there are a few sectoral legal provisions that limitedly promote that effect. A right to identity based on the TeF could fill that gap. It could be incorporated *in toto* into the Indian Constitution or it could be used as a vital and dynamic guiding principle in the implementation of digital identity law. This would not only make all digital identity stakeholders aware of their responsibilities, but also protect the future of digital identity in India.

9. Conclusion

This thesis focussed on determining how the legal regulation of digital identity could mirror the global nature of digital identity and simultaneously be compatible with national local difference.

To this end, the thesis first extensively examined the concept of digital identity.[1509] Here, it was determined that digital identity is a complex concept encompassing a range of forms and features, all sharing multiple subjective relationships with the individual.

Then, it analysed how local difference[1510] (which had thus far been sidelined in the digital identity regulatory discourse) affects digital identity using the UK and India as key jurisdictions in respect of the state of digital technologies and culture. Vast differences are evident between the UK and India in relation to the operating conditions, penetration, access and use of digital identity. Vast differences are also evident in how culture (i.e. attitudes, social values, norms and practices) impacts and affects digital identity. Culture influences how individuals relate to, express, use and protect their digital identities. This was established in the contexts like privacy, information sharing, communal use of personal information, authentication and verification, openness and transparency, anonymity and pseudonymity.

The thesis reviewed digital identity management,[1511] the industry self-regulatory solution for the creation, control and management of digital identities, which is globally marketed as a means of enabling digital identity subjects control their digital identities. Digital identity management emerges as a limited and incomplete tool for controlling digital identity. Additionally, in its core Western influences, assumptions and nature of development, it fails to account for the place of local difference.

[1509] **Ch 2**
[1510] **Ch 3**
[1511] **Ch 4**

Subsequently the thesis turned to the law. [1512] A comprehensive and contemporary comparative study of the law regulating digital identities in the UK and India was carried out. This substantiated that digital identity occupies diverse regulatory spaces. More vitally, this chapter provides evidence of how digital identity regulation in the UK and India shares both similarities and differences. (Recall, at the outset, vast differences were expected to emerge given the dissimilar nature of the two jurisdictions).

Specially designed case studies[1513] analysed the application of the law regulating digital identity in greater detail in relation to key digital identity aspects like privacy, sharing, reputation, anonymity, pseudonymity, access to Internet resources and control of personal data. These explicitly illustrate how difference manifests in the regulation of digital identity. Digital identity subjects in UK and India were shown to be on unequal footing in regards to the protection of their digital identity.[1514] The case studies also highlight the mismatch of digital identity law, local conditions and the *Volksgeist* in India.

Next the thesis, examined key national and international legal solutions proposed in respect of digital identity.[1515] The national legal proposals (Costa Rican right to virtual personality,[1516] Blackman's right to digital identity[1517] and Sullivan's right to database identity)[1518] were limited in scope and made problematic assumptions about the universality of the digital identity subject and its ability to control digital identity; something that the thesis has proved does not have global veracity.[1519] Thus they do not provide good models for regulation of digital identity in jurisdictions like India.

[1512] **Ch 5**
[1513] **Ch 6**
[1514] Here, the TeF can be used as a focal point of reference to expand consciousness of the role, duties and rights of digital identity stakeholders. The TeF can be used to facilitate the protection of the digital identity subject, give it explicit need based rights in and to its digital identity.
[1515] **Ch 7**
[1516] **Ch 7 (7.2.1)**
[1517] **Ch 7 (7.2.2)**
[1518] **Ch 7 (7.2.3)**
[1519] Nearly all of the legal solutions proposed are highly centred on the concept of the autonomous and private digital identity subject, who chooses, is able and willing to control its digital identity. They also presume that digital identity is privately zoned. They thus, fall short of proving to be useful to countries like India, due to their inflexibility in this respect.

Only De Hert's right to identity was found most appropriate in the context of the global implementation of digital identity and local difference.

In the final part,[1520] the thesis proposed the TeF as the solution to the central question of the thesis i.e. how the legal regulation of digital identity could mirror the global nature of digital identity and simultaneously be compatible with local difference. The TeF, recognising both the inevitability of international influences in the legal regulation of digital identity and the place of local difference, provides the answer. Finally, here is a solution that is internationally viable; grounded in local difference and particularly in the context of India, in its *Volksgeist.*

9.1. Broader significance

The broader significance of the thesis lies in three major respects: local embedding of law; significance of the TeF as a cultural communications framework and its international relevance.

9.1.1. Local Embedding of Law

While the law must take cognisance of international obligations in a globalised and interconnected world,[1521] it must also recognise that its relevance and impact lies at the core grassroots, local level. The law must, to be effectual, have local acceptance and validity. It must reflect inclusivity and integration of all digital identity stakeholders.[1522] This acceptance and validity comes more easily when law (whatever its origin) is grounded in the *local.* Law, that is a reflection of cultural and moral values of a community, is better received. In the digital identity context, this is particularly relevant because identity has a locally "constructed, relative and contingent character,"[1523] and digital identity is subject to local difference.

[1520] **Ch 8**

[1521] A key feature of which is permanence of nature. See AK Sahoo, *Sociological Perspectives on Globalisation* (Kalpaz, Delhi 2006), 238

[1522] It has been argued that law that has customary basis tends to have greater inclusivity. T Hanstad, RL Prosterman and R Mitchell, 'Poverty, Law and Land Tenure Reform,' in RL Prosterman, R Mitchell, T Hanstad (eds), *One Billion Rising: Law, Land and the Alleviation of Global Poverty* (Leiden University Press, Dordrecht 2009), 17- 56, 27

[1523] Jiri Priban, *Legal Symbolism: On Law, Time and European Identity* (Ashgate, Aldershot 2007), xi

This thesis is a call for greater recognition of the need to balance the reception of law in a legal community with a local tempering that makes the law effective and enables it to meet local needs. As stated, "there must be maintained a delicate and continuously adjusted equilibrium between law and cultural values of society, the one not lagging too far behind the other."[1524] This is one lesson India in particular would do well to take on board.

9.1.2. TeF as a Cultural Communications Framework

In its core, the TeF represents a vital conceptual framework that is rooted in the culture, history and spirit of the Indian people. It has great potential to be used by the Indian State to ground digital regulatory policy, revitalise it[1525] and provide it legitimacy in the light of local difference. Though several calls have been made for the localisation of digital law,[1526] the TeF is the first attempt to provide the terminology for this purpose. This is vital in the Indian context because though much of Indian law is a "hybrid conglomerate,"[1527] it is well accepted and evident that indigenous principles of law tend to find greater receptivity, acceptance and respect.[1528]

In this case the TeF could function as the *swadeshi*[1529] element in digital identity regulation. It could be employed by the Indian State to generate increased respect for official digital policies in a language that Indian digital identity subjects are familiar

---

[1524] MC Setalvad, 'Culture and Law,' in Raj Kumar (ed) *Essays on Legal Systems in India* (Discovery Publishing House, New Delhi 2003), 73-97, 80

[1525] JDM Derrett, *Religion, Law and the State in India* (OUP, Oxford 1999)

[1526] See S Akhtar and P Arinto (eds), *Digital Review of Asia Pacific 2009-2010* (Sage Publications, Delhi 2007), 277

[1527] Menski (2006) **n42**, 264

[1528] Menski (2006) **n42**, 265. Note also the comments of Kelly and Jones that "just as culturally inappropriate graphics, layout, design and rhetoric can confuse and repel target audiences, so can culturally inappropriate legal gaffes." Kendall Kelly and Jennifer Jones, 'Websites and the Law: An Avenue for Localization,' in Kirk St Amant (ed), *Linguistic and Cultural Online Communication Issues in the Global Age* (IGI Global, Hershey 2007), 202-211, 211

[1529] Meaning indigenous or home-grown. The *Swadeshi* Movement was popularised by MK Gandhi in the 1930's and still has contemporary relevance. See AT Hingorani (ed) *The Gospel of Swadeshi by MK Gandhi* (BVB, Mumbai 1967); V Sankaran Nair, *Swadeshi Movement* (Mittal Publishers, Delhi 1985). See also comments of Justice Krishna Iyer who calls for greater regard for "own legal ancestry." Justice VR Krishna Iyer, *The Indian Law: Dynamic Dimensions of the Abstract* (Universal Law Publishing, Delhi 2009), 10

with. This would lead to an increased affiliation to the law for digital identity stakeholders and for the Indian State a better ability to maintain law and order. At the same time, the TeF being of universal validity and accord with international legal principles would neatly avoid the tension that often results when local values and international values and law come up against each other. [1530]

9.1.3. The TeF and other jurisdictions

The TeF has relevance not only for India,[1531] but also for other jurisdictions[1532] like itself that ascribe greater value to duties over rights of the individual. For example, Confucian societies (e.g. China, Korea, Japan, Vietnam and Singapore) in East Asia[1533] and Islamic societies.[1534] Thus the placement of the duty element as the principal tenet of the TeF has great international appeal and might see countries other than those dominating the digital identity discourse (i.e. the digitally advanced West) take on this approach to digital identity regulation as it accords with their culture and philosophy.

[1530] Nahid Islam, *The Law of Non-Navigational Uses of International Watercourses* (Wolters Kluwer, Netherlands 2010), 38; Helen Stacy, *Human Rights for the 21st Century: Sovereignty, Civil Society, Culture* (SUP, Palo Alto 2009), 32

[1531] Hindu law over the ages and law in contemporary India recognise the ascendance of duties over rights. Aggarwal (2002) **n1451**, 58

[1532] The place of duties in Western legal jurisprudence is supported by theorists like Austin, Hart, MacCormick, Raz and Wellman. HLA Hart, 'Are There any Natural Rights?' (1955) 64 Philosophical Review, 175-191; Neil MacCormick, 'Children's Rights: A Test-Case for Theories of Rights,' in N MacCormick (ed) *Legal Right and Social Democracy: Essays in Legal and Political Philosophy* (Clarendon Press, Oxford 1982),154 -166; Neil MacCormick, 'Rights in Legislation,' in PMS Hacker and J Raz (eds), *Law, Morality and Society: Essays in Honour of HLA Hart* (Clarendon Press, Oxford 1977), 189. Joseph Raz, 'The Nature of Rights,' (1984) 93 Mind, 194-214; Joseph Raz, 'Legal Rights,' (1984) 4 OJLS, 1-21; Joseph Raz, 'Rights and Politics,' in J Tasioulas (ed), *Law, Values and Social Practices* (Aldershot, Dartmouth 1997), 75. Raz postulated that one's interests were protected by duty. Carl Wellman, *A Theory of Rights* (Rowman and Allanheld, NJ 1985); Carl Wellman, *Real Rights* (OUP, NY 1995); Carl Wellman, *The Proliferation of Rights: Moral Progress or Empty Rhetoric?* (Westview Press, Colorado 1999). Wellman believed that the essence of a right was to have choice or control over the corresponding duty.

[1533] Hidetoshi Hashimoto, *The Prospects for a Regional Human Rights Mechanism in East Asia* (Taylor and Francis, London 2003), 50; Lee Manwoo, 'North Korea and the Western Notion of Human Rights,' in JC Hsiung (ed) *Human Rights in East Asia: A Cultural Perspective* (Paragon, NY 1985), 129-151

[1534] AM Mutahari, 'Primary Principles of Law in Islam,' in OICC, *Islamic Views on Human Rights: Viewpoints of Iranian Scholars* (Alhoda, Tehran 2001), 179-190, 186

9.2. Future directions

This thesis and its results are particularly significant for India and will continue to be as digital identity implementation grows and pervades every aspect of life. Specifically, the TeF presents a basis for critical analysis of the Indian UID scheme.[1535] To date, no framework has been developed for the critical analysis of a scheme that will affect the lives of over a billion of the world's population and be the largest of its kind in the world.[1536] The TeF in its three elements represents a good framework to evaluate the scheme and its effects.

The evaluatory exercise could ask the following questions on the basis of the core aspects of the TeF. First, does the Scheme promote a duty to respect digital identity by all stakeholders? Next, does the Scheme establish and sufficiently prescribe the conditions and circumstances under which digital identity under the Scheme might be enjoyed and legitimately restricted? Does it prescribe lawful procedure in this respect? Finally, if a person is denied a digital identity under the Scheme, does it provide recourse to an appropriate and effective remedy? This exercise would be in the best interests of not just Indian digital identity subjects but all stakeholders of the Scheme.

Given that the Indian digital identity subject has no effective right to digital identity, unlike digital identity subjects in the EU and the UK, it might be worthwhile to explore further how the TeF might be incorporated as a legal right into the Indian legal system. A step in this direction might be to examine whether the TeF could be framed as a constitutional right in India. All three elements of the TeF fit well into the Indian constitutional setting. First, the role of duties is explicitly recognised under the Constitution. The second element (non-deprivation of digital identity except according to procedure established by law also finds substantial support, particularly as reflected in the language of Article 21 (the right to life). There is also

---

[1535] **Ch 4 (4.3, para 7); Ch 5 (5.2.3.2)**

[1536] J Joseph, 'How the UID Project Can Be a Cause for Concern,' *CNN-IBN* (5 October 2010) <http://ibnlive.in.com/news/how-the-uid-project-can-be-a-cause-for-concern/132375-3.html>; S Sharma, 'Crisis for Identity or Identity Crisis?' *D-sector.org* (12 October 2010) <http://www.d-sector.org/article-det.asp?id=1396>

strong constitutional support for the place of remedies, the final element of the TeF, as in Articles 32 and 226 of the Constitution.

9.3. Closing thought

Tagore[1537] commented, "You can't cross the sea merely by standing and staring at the water." This thesis has taken on this exhortation and attempted in its comparative legal exercise to cross a choppy digital identity regulatory sea and has come out, on the other side, in tow with perhaps not the 'ultimate' model for digital identity regulation but a viable and useful basis on which the legal regulation of digital identity can mirror the global nature of digital identity and be compatible with local difference.

[1537] R Tagore, Indian Poet, Playwright and Essayist. Nobel Laureate (Literature) (1913)

REVISITING THE LEGAL REGULATION OF DIGITAL IDENTITY IN THE LIGHT OF GLOBAL IMPLEMENTATION AND LOCAL DIFFERENCE

Rowena Edwardina Rodrigues

Doctor of Philosophy
University of Edinburgh
2011

Appendix A

Author's thesis related publications and presentations

Book Chapters

1. R Rodrigues, 'User Control Problems and Taking User Empowerment Further,' in V Matyáš, S Fischer- Hübner, D Cvrcek, Petr Svenda (eds), *The Future of Identity*, IFIP AICT 298 (Springer, Germany 2009), 211-225
2. R Rodrigues, 'Digital Identity and Anonymity: Desi Manifestations and Regulation,' in S Fischer-Hübner, P Duquenoy, A Zuccato & L Martucci (eds), *The Future of Identity in the Information Society*, IFIP Vol. 262, (Springer, Boston 2008), 359–374

Book Reviews

1. R Rodrigues, 'The Future of Identity in the Information Society: Challenges and Opportunities,' Book Review, 2009 (2) Journal of Information, Law & Technology <http://go.warwick.ac.uk/jilt/2009_2/rodrigues>

Presentations

1. R Rodrigues, 'Identity and Privacy: Sacred Spice and All that's Nice,' GikII V, Edinburgh (28-29 June 2010)
2. R Rodrigues, 'Learning From Each Other: Digital Identity Management and Regulation Principles for India and the UK,' Invited Talk, INDIA SIM 2009, Security and Identity Management, Bangalore India (22-23 January 2009)
3. R Rodrigues, 'The User and the Quandary of Control,' FIDIS/IFIP Internet Security & Privacy Summer School, Masaryk University, Czech Republic (1-7 September 2008)
4. R Rodrigues, 'Digital Identity, Anonymity, Pseudonymity and Law in India,' IFIP Summer School on the Future of Identity in the Information Society, University of Karlstad, Sweden (6-10 August 2007)

Bibliography

International Legal Instruments

1. Agreement on Trade Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C (15 April 1994) 33 ILM 1197 **(The TRIPS Agreement)**
2. Berne Convention for Protection of Literary and Artistic Works (9 September 1886) 828 UNTS 221
3. Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS xvi
4. Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (29 October 1971) 866 UNTS 71
5. Convention on the Prevention and Punishment of the Crime of Genocide (adopted 9 December 1948, entered into force 12 January 1951) 78 UNTS 277
6. Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 **(UNCRC)**
7. Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite (21 May 1974) <http://www.wipo.int/treaties/en/ip/brussels/pdf/trtdocs_wo025.pdf>
8. Declaration of the Rights of the Child (20 November 1959) UNGA Res. 1386 (XIV), 14 UN GAOR Supp. (No. 16) 19, UN Doc A/4354
9. Declaration on the Protection of All Persons from Enforced Disappearance, (18 December 1992), UN Doc A/47/49
10. International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (26 October 1961)
11. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 **(ICCPR)**
12. International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 999 UNTS 3 **(ICESCR)**
13. The Universal Copyright Convention (6 September 1952) <http://portal.unesco.org/en/ev.php-URL_ID=15381&URL_DO=DO_TOPIC&URL_SECTION=201.html>
14. UNCITRAL Model Law on Electronic Commerce (adopted 12 June 1996) <http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf>
15. UNCITRAL Model Law on Electronic Signatures 2001 (adopted 5 July 2001) <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf>
16. United Nations Millennium Declaration (8 September 2000), UN Doc A/55/49 (2000)
17. Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A (III) **(UDHR)**
18. WIPO Copyright Treaty (adopted 20 December 1996, entered into force 6 March 2002) 36 ILM 65 (1997) **(WCT)**

19. WIPO Performances and Phonograms Treaty (adopted 20 December 1996, entered into force 20 May 2002) 36 ILM 76 (1997) **(WPPT)**
20. WSIS Geneva Declaration of Principles, WSIS-03/GENEVA/DOC/4-E (12 December 2003), Document WSIS-03/GENEVA/DOC/4-E <http://www.itu.int/wsis/docs/geneva/official/dop.html>

Regional Instruments

Europe

1. Charter of the Fundamental Rights of the European Union (18 December 2000) OJ C 364/01
2. Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 04 November 1950, entered into force 03 September 1953) 213 UNTS 221 **(European Convention on Human Rights, as amended/ECHR)**
3. Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts OJ L 095, 21/4/1993, P 0029 - 0034
4. Council of Europe Convention on Cybercrime (adopted 23 November 2001, entered into force 7 January 2004), CETS No 185
5. Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community Framework for Electronic Signatures, OJ L 013, 19/01/2000 P 0012 – 0020 **(Electronic Signatures Directive)**
6. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, OJ L 178, 17/07/2000, P 0001-0016 (**Directive on Electronic Commerce)**
7. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society OJ L 167, 22/06/2001, P 0010-0019 (**Information Society Directive)**
8. Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities OJ L 108, 24/04/2002, P 21-32 (**Access Directive)**
9. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services OJ L 108, 24/04/2002, P 33-50 **(Framework Directive)**
10. Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, OJ L 108, 24/04/2002, P 51-77 (**Universal Service Directive**)
11. Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector OJ L 201, 31/07/2002, P 0037 – 0047 (**Directive on Privacy and Electronic Communications)**

12. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, OJ L 105, 13/04/2006, P 54-63
13. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data OJ L 281, 23/11/1995, P 0031-0050 (**The Data Protection Directive**)
14. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector OJ L 24, 30/01/1998, P 1-8 (**Telecommunications Data Protection Directive**)
15. Treaty on the European Union OJ C 191 (29 July 1992)

National Legislation

UK

Legislation (Public Acts & Statutory Instruments)

1. Civic Government (Scotland) Act 1982 (c.45)
2. Communications Act 2003 (c.21)
3. Companies Act 1985 (c.6)
4. Computer Misuse Act 1990 (c.18)
5. Copyright, Designs and Patents Act 1988 (c.48)
6. Coroners and Justice Act 2009 (c.25)
7. Criminal Justice and Immigration Act 2008 (c.4)
8. Defamation Act 1952 (c.66)
9. Defamation Act 1996 (c.31)
10. Digital Economy Act 2010 (c.24) (**DEA 2010)**
11. Electronic Communications Act 2000 (c.7) (**ECA**)
12. Electronic Signatures Regulations 2002 (SI No 318) (**ESR)**
13. Emergency Registration Act 1939
14. European Communities Act 1972 (c.68)
15. Forgery and Counterfeiting Act 1981 (c.45)
16. Fraud Act 2006 (c. 35)
17. Freedom of Information (Scotland) Act 2002 (asp 13)
18. Freedom of Information Act 2000 (c.36)
19. Human Rights Act 1998 (c.42) (**HRA 1998)**
20. Identity Cards Act 2006 (c.15)
21. Identity Documents Act 2010 (c.40)
22. Magna Carta 1297 (c.9)
23. National Registration Act 1939
24. Obscene Publications Act 1959 (c.66)
25. Obscene Publications Act 1964 (c.74)
26. Patents Act 1977 (c.37)

27. Police and Justice Act 2006 (c.48)
28. Protection of Children Act 1978 (c.37)
29. Public Order Act 1986 (c.64)
30. Race Relations Act 1976 (c.74)
31. Representation of the People (England and Wales) (Amendment) Regulations 2001 (SI No 1700)
32. Representation of the People (England and Wales) Regulations 2001 (SI 341)
33. Representation of the People Act 1983 (as amended by Representation of the People Act 2000) (c.2)
34. Scotland Act 1998 (c.46)
35. Sexual Offences Act 2003 (c.42)
36. The Data Protection Act 1998 (Commencement) Order 2000 (SI No 183, c.4)
37. The Consumer Protection (Distance Selling) Regulations 2000 (SI No 2334)
38. The Copyright (Computer Programs) Regulations 1992 (SI No 3233)
39. The Copyright and Related Rights Regulations 2003 (SI No 2498)
40. The Criminal Justice (Northern Ireland) Order 1996
41. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 (SI No 31)
42. The Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI No 417)
43. The Data Protection (Processing of Sensitive Personal Data) Order 2006 (SI No 2068)
44. The Data Protection Act 1998 (c.29) (**DPA 1998)**
45. The Data Protection Tribunal (National Security Appeals) (Telecommunications) Rules 2000 (SI No 731)
46. The Data Retention (EC Directive) Regulations 2009 (SI No 859)
47. The Information Tribunal (Enforcement Appeals) (Amendment) Rules 2005 (SI No 450)
48. The Information Tribunal (Enforcement Appeals) Rules 2005 (SI No 14)
49. The Information Tribunal (National Security Appeals) Rules 2005 (SI No 13)
50. The Police and Criminal Evidence (Northern Ireland) Order 1989 (SI No 408)
51. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI No 2426)
52. The Unfair Terms in Consumer Contracts Regulations 1999 (SI No 2083)
53. Theft (Northern Ireland) Order 1978 (SI No 1407, NI 23)
54. Theft Act (Northern Ireland) 1969 (c. 16)
55. Theft Act 1968 (c. 60)
56. Theft Act 1978 (c. 31)
57. Trade Marks Act 1994 (c.26)

India

1. Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules 2003
2. Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002
3. Information Technology (Karnataka) Rules 2004 (5 August 2004), <http://www.ccaoi.in/UI/docs/Karnataka%20Cyber%20Cafe%20Regulations.doc>
4. Rajasthan Cyber Café Rules 2007, <http://www.rajasthan.gov.in/rajgovresources/newitems/Raj_Cyber_Cafe_Rules.pdf>
5. Rules for Licensing and Controlling Places of Public Amusement (other than Cinemas) and Performances for Public Amusement including Pool Game Parlours, Amusement Parlours Providing Computer Games, Virtual Reality Games, Cyber Cafes, Games with Net, Internet or Intranet Connectivity, Bowling Alleys, Card Rooms, Social Clubs, Sports Clubs, Cabaret performances, Discotheque, Games, Melas and Tamashas (First Amendment) Rules, 2006 (Mumbai), <http://www.mumbaipolice.org/downloads/Notification%20of%20Cyber%20Cafe.pdf>
6. Telecom Consumers Protection and Redressal of Grievances Regulations, 2007 (3 of 2007)
7. The Browsing Centre (Tamil Nadu) Rules/Conditions, <http://www.tnpolice.gov.in/forms/BROWSINGCENTREREGULATIONRULESANDAPPLICATION.pdf>
8. The Citizenship Act 1955 (Act 57 of 1955)
9. The Code of Criminal Procedure 1973 (Act 2 of 1974) **(CrPC)**
10. The Constitution of India
11. The Copyright (Amendment) Act 1999 (Act 49 of 1999)
12. The Copyright Act 1957 (Act 14 of 1957)
13. The Evidence Act 1872 (Act 1 of 1872)
14. The Gujarat Information Technology Rules 2004, <http://www.ccaoi.in/UI/docs/Cyber%20Law%20-%20Guj.pdf>
15. The High Courts (Seals) Act 1950 (Act 7 of 1950)
16. The Indian Contract Act 1872 (Act 9 of 1872) (**ICA)**
17. The Indian Penal Code 1860 (Act 45 of 1860) (**IPC)**
18. The Information Technology (Amendment) Act 2008 (Act 10 of 2009) (**ITAA 2008**)
19. The Information Technology (Certifying Authorities) Regulations 2001
20. The Information Technology (Certifying Authorities) Rules 2000
21. The Information Technology Act 2000 (Act 21 of 2000) (**ITA 2000**)
22. The National Identification Authority of India Bill, 2010 <http://uidai.gov.in/documents/NIA%20Draft%20Bill.pdf>
23. The Registration of Births and Deaths Act 1969 (Act 18 of 1969)
24. The Representation of People Act 1950 (Act 43 of 1950)
25. The Sikkim Information Technology Rules 2009

26. The State Emblem of India (Prohibition of Improper Use) Act 2005 (Act 50 of 2005)
27. The Succession Act 1865 (Act 10 of 1865)
28. The Transfer of Property Act 1882 (Act 4 of 1882)
29. Trademarks Act 1999 (Act 47 of 1999)

US

1. The Constitution of the United States (**US Constitution**)
2. The Electronic Signatures in Global and National Commerce Act Pub.L. 106-229, 114 Stat 464 (2000) (**ESIGN**)
3. The Uniform Electronic Transactions Act 1999 (**UETA**)

Bermuda

The Electronic Transactions Act 1999 (26 of 1999)

Costa Rica

Congress of the Republic of Costa Rica, Constitutional Reform for the Protection of the Virtual Personality as a Fundamental Right, Law Bill, Congresswoman M I Zamora Castillo, Expedient No. 15890 (9 May 2005); Spanish version, <http://virtualrights.org/PROYECTO%20PERSONALIDAD%20VIRTUAL.doc>

Cases and Decisions

European Court of Justice

Bodil Lindqvist [2004] 1 CMLR 20

European Court of Human Rights

A v United Kingdom (1999) 27 EHRR 611
Abdulaziz, Cabales & Balkandali v UK (1985) 7 EHRR 471
AG (Eritrea) [2007] EWCA Civ 801
Airey v Ireland (1979) 2 EHRR 305
Akdeniz v Turkey ECtHR, App 25165/94 (31 May 2001)
Amann v Switzerland (2000) 30 EHRR 843
Artico v Italy (1980) 3 EHRR 1
August v UK (2003) 36 EHRR CD 115
Bensaid v the United Kingdom (2001) 33 EHRR 10
Buckley v UK (1996) 23 EHRR 101
Burghartz v Switzerland (1994) 18 EHRR 101

Case of L v Lithuania ECtHR, App 27527/03 (11 September 2007)
Christine Goodwin v The United Kingdom ECtHR, App 28957/95 (11 July 2002)
Copland v UK (2007) 45 EHRR 37
Daróczy v Hungary ECtHR, App 44378/05 (1 July 2008)
Deep Vein Thrombosis (2002) EWCH 2825 (QB)
Dodov v Bulgaria EctHR, App 59548/00 (17 January 2008)
Dudgeon v United Kingdom 4 EHRR 149 (merits) (1981)
Dudgeon v United Kingdom 5 EHRR 573 (just satisfaction) (1983)
Edwards v United Kingdom (2002) 35 EHRR 19
Fuentes Bobo v Spain, ECtHR, App 39293/98 (29 February 2000)
Gaskin v the United Kingdom (1990) 12 EHRR 36
Golder v United Kingdom (1975) 1 EHRR 524
Goodwin, Klass v Germany (1978) 2 EHRR 214
Guerra v Italy (1998) 26 EHRR 357
Halford v UK 24 EHRR 523 (1997)
Hatton v United Kingdom (2003) 37 EHRR 611
Herczegfalvy v Austria 15 EHRR 437 (1992)
Ilhan v Turkey ECtHR, App 22277/93 (18 May 2000)
Ivison v UK (2002) 35 EHRR CD 20
Jaggi v Switzerland ECtHR, App 58757/00 (13 July 2006)
Jordan v United Kingdom (2003) 37 EHRR 2
KA and AD v Belgium ECtHR, Apps 42758/98 and 45558/99 (17 February 2005)
Keenan v United Kingdom (2001) 33 EHRR 913
Khan v the United Kingdom (2001) 31 EHRR 45
LCB v United Kingdom (1999) 27 EHRR 212
Leander v Sweden (1978) 2 EHRR 214
Malone v UK (1984) 7 EHRR 14
MC v Bulgaria [2003] ECHR 646
Menson v UK (2003) 37 EHRR CD 220
Messina v Italy ECtHR, App 13803/88 (26 February 1993)
Odievre v France (2004) 38 EHRR 43
Őneryildiz v. Turkey (2004) 39 EHRR 12
Osman v United Kingdom (2000) 29 EHRR 245
Özgür Gündem v Turkey ECtHR, App 23144/93 (16 March 2000)
Peck v the United Kingdom (2003) 36 EHRR 41
PG & JH v the United Kingdom [2000] ECHR 192
Pretty v the United Kingdom (2002) 35 EHRR 1
Rotaru v Romania ECtHR, App 28341/95 (4 May 2000)
S and Marper v the United Kingdom [2008] ECHR 1581
Segerstedt-Wiberg v Sweden [2007] EHRR 2 (CCHR)
Smirnova v Russia (2004) 39 EHRR 450
Steel & Morris v United Kingdom (2005) 41 EHRR 22
Stjerna v Finland 24 EHRR 195 (1994)
Storck v Germany (2005) 43 EHRR 96
Stubbings v UK (1996) 23 EHRR 213
Tarariyeva v Russia EctHR, App 4353/03 (14 December 2006)
TP v United Kingdom (2002) 34 EHRR 2
Vo v France (2005) 40 EHRR 12

Von Hannover v Germany (2005) 40 EHRR 1
Winer v UK 48 DR 154 (1986)
X & Y v Netherlands (1985) 8 EHRR 235
Z v the United Kingdom [2001] 2 FLR 612

Other European Decisions

College van Burgemeester en Wethouders van Rotterdam v MEE Rijkeboer Netherlands, Case C-553/07, OJ C 153 (04 July 2009)
Commission v Grand Duchy of Luxembourg [2001] ECR I-07069
European Commission supported by European Data Protection Supervisor v Federal Republic of Germany, Case C-518/07 OJ C 113 (01 May 2010)
European Commission v Federal Republic of Germany OJ C 283 (24 November 2007)
Heinz Huber v Bundesrepublik Germany, Case C-524/06 OJ C 44 (21 February 2009)

Australia

Adam Kaplan v Go Daddy Group Inc [2005] NSWSC 636
Cullen v White (2003) WASC 153
Gutnick v Dow Jones & Co Inc [2001] VSC 305
Rindos v Hardwick, Supreme Court of Western Australia, (unreported), 31 March 1994
The Buddhist Society of Western Australia Inc v Bristile Ltd & Anor [2000] WASCA 210

France

Lefebure v Lacambre 55181/98, No. 1/JP

Germany

Volkszählungsurteil decision by the German Federal Constitutional Court (*Bundesverfassungsgericht*) in 1983, BVerfGe 65, 1 <http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm>

India

A and B v The State of NTC of Delhi Crl MC 283/2009
Acqua Minerals Ltd v Shailesh Gupta 2002 (24) PTC 35 (Del)
AIIMS Students' Union v AIMS (2002) 1 SCC 428

AK Gopalan v The State of Madras 1950 SCR 88
Alika Khosla v Thomas Mathew (2002) 62 DRJ 851
Anil Hada v Indian Acrylic Ltd (2000) 1 SCC 1
Anuradha Kshirsagar v State of Maharashtra 1991 CriLJ 410
Arun Ghosh v State of West Bengal [1970] 1 SCC 98
AS Zingthan v State of Manipur AIR 1998 Gau 102
Athletes Foot Marketing Adm Inc v Cobra Sports Limited 1980 RPC 343
Avnish Bajaj v State Crl MC 3066/2006 (Del)
Bai Gulab v Jivanlal Harilal (1922) 24 BOMLR 5
Basheshar Nath v Commissioner of Income Tax 1959 AIR 149
Bennet Coleman and Co Ltd v Union of India 1973 AIR 106
Bhekha Ahir v Emperor AIR 1947 Pat 236 (G)
Bhikubai Meher v Hariba Meher (1925) 27 BOMLR 13
Bodhisattwa Gautam v Subhra Chakraborty AIR 1996 SC 922
Cadila Health Care Ltd v Cadila Pharmaceuticals Ltd (2001) SCL 534
Cheria P Joseph v Prabhakarn AIR 1967 Kar. 234
Dabur India Ltd v M/S Colortek Meghalaya Pvt Ltd CS (OS) 2029/2009 (Del)
Diljeet Titus v Alfred Adebare 130 (2006) DLT 330
District Registrar and Collector v Canara Bank CA 6350-6374/1997 (SC)
District Registrar and Collector, Hyderabad v Canara Bank (2005) 1 SCC 496
DM Entertainment v Jhaveri Case 1147/2001 (Del)
Dr PR Ramanujam v IGNOU 25 September 2006 (Delhi High Court)
Dr. Reddy's Laboratories Ltd v Manu Kosuri 2001 PTC 859 (Del)
Ellora Industries v Banarsidas Goel AIR 1980 Del 254
Express Newspapers v Union of India (1985) 1 SCC 641
Francis Coralie Mullin v The Administrator, Union Territory of Delhi 1981 SCR (2) 516
Gagan Raj Singh Nagori v Union of India 1979 WLN 634
Goona Durgaprasada Rao v Goona Sudarsanaswami (1940) 1 MLJ 800 (Chennai)
Govind Das v Bishambhar Das (1917) ILR 39 All 561
Govind v State of MP (1975) 2 SCC 148
Gremach Infrastructure Equipments & Projects Limited v *Google India Private Limited* CS 506/2008, 18 Feb 2008 (Bom)
GS Walavalkar v PS Rege AIR Bom 224
Hindustan Radiators Co v Hindustan Radiators Ltd AIR 1987 Del 353
Infosys Technologies Limited v Pravarthan Infosys Pvt Ltd Delhi High Court, 20 Feb 2006
Intel Corporation v S Ramanan 2002 (25) PTC 457 Mad
John Richard Brady v Chemical Process Equipments AIR 1987 Delhi 372
Kharak Singh v State of UP (1964) 1 SCR 332
Khushwant Singh v Maneka Gandhi AIR 2002 Del 58
Kirloskar Proprietary Ltd v Kirloskar Dimensions AIR 1997 Karnataka 1
Kishore Zarda Factory (P) Ltd v JP Tobacco House AIR 1999 Delhi 172
KJ Doraisamy v The Assistant General Manager WP 17761/2006 (Chennai High Court)
Klaus Mittelbachert v East India Hotels Ltd AIR 1997 Del 201
Lakshmi Ganesh Films v Government of AP 2006 (4) ALD 374

M/s Makkal T Thodarpu Kuzhuman Ltd v Mrs V Muthulakshmi CRP (PD) 3299/2007 (Mad)
Maneka Gandhi v Union of India (1978) 1 SCC 248
Manisha Koirala v Shashilal Nair 2003 (2) BomCR 136
Mars Incorporated v Chanda Softy Ice Cream AIR 2001 Madras 237
Maruti Shripati Dubal v State of Maharashtra 1987 (1) BomCR 499
Mattel Inc and Ors v Jayant Agarwalla CS (OS) 344/2008, 17 Sept 2008 (Delhi High Court)
MC Mehta v Union of India AIR 1988 SC 1037
MH Hoskot v State of Maharashtra AIR 1978 SC 1548
Michael HN Johnson v Subhash Chandra 60 (1995) DLT 757
Microsoft Corporation v A Jain CS (OS) 967/2007(Del)
Microsoft Corporation v Akram Khan CS (OS) 117/2003(Del)
Microsoft Corporation v Deepak Chandwani, Unreported ex parte interim injunction order, Suit 1680/99 (Del)
Microsoft Corporation v Deepak Raval 2006 (33) PTC 122 (Del)
Microsoft Corporation v K Mayuri 2007 (35) PTC 415 (Del)
Microsoft Corporation v Kamal Vahi CS (OS) 817/2004 (Del)
Microsoft Corporation v Kiran 2007 (35) PTC 748 (Del)
Microsoft Corporation v Rahul Pachpore CS (OS) 2428/1999 (Del)
Microsoft Corporation v Rajender Pawar CS (OS) 530/2003 (Del)
Microsoft Corporation v Yogesh Popat 2005 (30) PTC 245 (Del)
MK Chandran v Commr of Police, Kochi AIR 1998 Ker 347
MP Sharma v Satish Chandra AIR 1954 SC 300
MP State Co-op Dairy Federation Ltd. v RK Jaminder (2009) 15 SCC 221
Mr 'X' v Hospital 'Z' (1998) 8 SCC 296
Mrs. Shanta v State of AP AIR 1998 AP 51
Ms X v Mr Z 96 (2002) DLT 354
Nasscom v Ajay Sood 2005 (30) PTC 437
Noor Mohammed v Mohammed Jiajdin 1991 (0) MPLJ 530
NR Dongre v Whirlpool Corporation (1996) 5 SCC 714
Olga Tellis v Bombay Municipal Corporation 1986 AIR 180
Om Kumar v Union of India (2001) 2 SCC 386
Parami Ramayya v Mahadevi Shankarappa (1910) 12 BOMLR 196
People's Union for Civil Liberties v Union of India (1997) 1 SCC 301
Petronet LNG Ltd v Indian Petro Group CS (OS) 1102/2006, 22 April 2009 (Delhi High Court),
Phoolan Devi v Shekhar Kapoor 57 (1995) DLT 154
R Govinda Rao v Director, National Institute of Technology 2006 (2) ALD 152
R Rajagopal v State of Tamil Nadu AIR 1995 SC 264
Ram Jethmalani v Subramaniam Swamy AIR 2006 Delhi 300
Ramjilal Modi v State of UP AIR 1957 SC 620.
Rediff Communication Ltd v Cyberbooth 1999 (3) All MR 164 (Bom)
Rohtas Industries Ltd. v Rohtas Industries Staff Union AIR 1976 SC 425
Romesh Thapar v Madras AIR 1950 SC 124
Roshan Lal Oil Mills Ltd v Assam Co Ltd 1996 (16) PTC 699
RS Barolia v Commandant SRP (10 February 1999) (Gujarat High Court)
RSEB v Jai Singh AIR 1997 Raj 141

Sakal Newspapers v Union of India AIR 1973 SC 112
Satyam Infoway Ltd v Sifynet Solutions CA 028/2004 (SC)
Sharda v Dharampal (2003) 4 SCC 493
Sheo Ratan Agarwal v State of MP (1984) 4 SCC 352
Shri ASN Deekshitulu v State of Andhra Pradesh 1996 AIR 1765 (SC)
SK Wodeyar v Ganapati Dixit (1935) 37 BOMLR 584
SMC Pneumatics (India) Pvt Ltd v Jogesh Kwatra CS 1279/2001 (Del)
Socieadade de Fomento Industrial Pvt Ltd v Sebastian (Sebi) Rodrigues CS 265/2008 (Kol)
Spring Meadows Hospital v Harjot Ahluwalia (1998) 4 SCC 39
SR Bommai v Union of India (1994) 3 SCC 1
State of Gujarat v Mirzapur Kassab [2005] RD-SC 602
State of Punjab v Major Singh 1966 SCR (2) 286
State of Tamil Nadu v Suhas Katti CC No. 4680/2004 5 November 2004 (AMM, Egmore)
Swami Nithyanandaji Maharaj Case, CS 346/2010 (Chennai High Court)
Tata Sons Ltd v Manu Kosari 2001 PTC 432 (Del)
The Managing Director v Mrs V Muthulakshmi CRP (PD) 3299/2007 (Chennai High Court)
Titan Industries Ltd v Prashant Koapati, Interloc Interim App 787/1998, CS 179/1998 (Delhi High Court)
UJ Chiang v Global Broadcast News 2008 (2) BomCR 400
Union of India v Naveen Jindal AIR 2004 SC 1559
UP Pollution Control Board v Messers Modi Distillery (1987) 3 SCC 684
Vaman Deshpande v Krishnaji Kulkarni (1919) 21 BOMLR 427
Vimal CJ Jain v Shri Pradhan 1979 AIR 1501
Virender v State of NCT of Delhi Crl A No 121/2008
Yahoo! Inc v Akash Arora & Anr 1999 PTC (19) 201
Yahoo, Inc v Sanjay V Shah 128 (2006) DLT 488
Zee Telefilms Ltd v Union of India AIR 2005 SC 2677
Zee Telefilms v Sundial Communications 2003(5) BomCR 404

New Zealand

Hosking and Hosking v Runting and Pacific Magazines NZ Ltd (2005) 1NZLR 1

UK

1-800-Flowers Inc v Phonenames Ltd [2001] EWCA Civ 721
A v B plc [2003] QB 195
Andrews v Ramsay [1903] 2 KB 635
Applause Store Productions Ltd and Firsht v Raphael [2008] EWHC 1781 (QB)
Argyll v Argyll [1967] Ch 302
Blythe v Birmingham Waterworks (1856) 11 Exch 781
Bonnier Media Ltd v Smith 2002 SCLR 977
Bourhill v Young [1943] AC 92

British Medical Association v Marsh (1931) 48 RPC 565
British Telecommunications Plc v One In A Million Ltd [1999] 1 WLR 903
Cambell v MGN [2004] UKHL 22
Carrick Jewellery Ltd v Ortak 1989 GWD 35-1624
Christopher John Quinton v Robin H Peirce [2009] EWHC 912 (QB).
Clark v Associated Newspapers [1998] RPC 261
Coco v AN Clark (Engineers) Ltd [1969] RPC 41
Direct Line Group Limited v Direct Line Estate Agency Limited [1997] FSR 374
Donoghue v Stevenson [1932] AC 562,580
Douglas v Hello! [2005] EWCA CIV 595
Durant v FSA [2003] EWCA Civ 1746
Easyjet Airline Co v Tim Dainty [2002] FSR 6
Ellerman Investments Limited v Elizabeth C-Vanci [2006] EWHC 1442 (Ch)
Elvis Presley Enterprises Inc v Sid Shaw Elvisly Yours [1999] RPC 567
Erven Warnink v Townend [1979] AC 731
Euromarket Designs Incorporated v Peters & Anr [2000] EWHC Ch 179
Glaxo v Glaxowellcome Limited [1996] FSR 388
Global Projects Management Ltd v Citigroup Inc and Ors [2005] EWHC 2663 (Ch)
Global Projects Management Ltd v Citigroup Inc and Others [2006] FSR 39
Godfrey v Demon Internet Service [2001] QB 201
Goodwill v British Pregnancy Advisory Service [1996] 2 All ER 161
Haley v London Electricity Board [1965] AC 778
Harford v Swiftrim [1987] ICR 439
Hines v Winnick [1947] Ch 708
Imageview Management Ltd v Jack [2009] EWCA Civ 63
JH Rayner Ltd. v Dept. of Trade & Industry (1990) 2 AC 418 HL
Jim Murray v Jonathan Spencer 20 May 2002, Lincoln County Court (Internet libel)
John Haigh and Co Ltd v John DD Haigh Ltd 1957 SLT (Notes) 36
John Walker and Sons Ltd v Henry Ost & Co Ltd [1970] RPC 489
Joyce v Sengupta [1993]1 All ER 897
Kaye v Robertson [1991] FSR 62 (CA)
Kean v McGivan [1982] FSR 119
Keith-Smith v Williams [2006] EWHC 860 (QB)
LB (Plastics) Ltd v Swish Products Ltd [1977] FSPLR 87
Lochgelly Iron and Coal Co v McMullan [1934] AC 1 at 25
Loutchansky v Times Newspapers [2001] EWCA Civ 536 (Internet libel)
Maxim's Ltd v Dye [1977] FSR 364
McCarthys Ltd v Smith [1979] 3 All ER 325
McKennitt v Ash [2006] EWCA Civ 1714
Metropolitan International Schools Ltd v Designtechnica Corporation and Ors [2009] EWHC 1765 (QB)
Murray v Big Pictures (UK) Ltd [2008] EWCA Civ 446 (07 May 2008)
Napier v Pressdram Ltd [2009] EWCA Civ 443
Nichols Plc v Registrar of Trademarks [2005] All ER (EC) 1
Padmore v IRC [1989] STC 493
Palsgraf v Long Island Railroad Co (1928) 248 NY 339
PC Products v Dalton [1957] RPC 199
Per Burford's Application (1919) 36 RPC 139, 150

Phones4U Ltd v Phone4u.co.uk Ltd [2006] EWHC Civ 244
R v Breakwell [2009] EWCA Crim 2298
R v Gold [1988] 2 All ER 186
R v Lyons (2002) UKHL 44
R v Scott [2008] EWCA Crim 3201
Ravencroft v Herbert (1980) RPC 103
Reckitt and Coleman Products v Borden Inc [1990] RPC 341
Regina v Secretary of State for Culture, Media and Sport [2008] 1 AC 1312
Reuter v Muhlens (1953) 70 RPC 235
Rhodes v Macalister (1923) 29 Com Cas 19.
Robertson v Newsquest 2006 SCLR 792 (repetitive libel)
Robertson v Wakefield Metropolitan Council [2001] EHC Admin 915
Rowland v Mitchell (1897) 14 RPC 37
Society of Accountants in Edinburgh v Corporation of Accountants (1893) 20R 750
Speechworks Limited v Speechworks International Incorporated [2000] ScotCS 200
The Author of a Blog v Times Newspapers Ltd [2009] EWHC 1358 (QB)
Thistle v Thistle Telecom Ltd 2000 SLT 262
Thoburn v Sunderland City Council [2002] 3 WLR 247
Thornton v Shoe Lane Parking [1971] 2 QB 163
Totalise Plc v Motley Fool [2001] EWCA Civ 1897
Treadwell's Drifters Inc v RCL Ltd 1996 SLT 1048
Urbanski v Patel (1978) 84 DLR (3rd) 650
Walter v Lane (1990) AC 539
Worthing RFC Trustees v IRC [1987] 1 WLR 1057
X (HA) v Y [1988] 2 All ER 648

USA

Barrett v Fonorow 112 Cal App 4th 749 (2003)
*Barrett v Rosenthal*112 Cal App 4th 749 (2003)
Bell v Mich. Council 25 of Am. Federation of State, County, Municipal Employees. No. 246684, 2005 WL 356306 (Mich Ct App, 15 February 2005)
Cubby, Inc v CompuServe Inc 776 F. Supp. 135 (SDNY 1991)
In the Matter of Microsoft Corp, FTC Docket No. C-4069 (20 Dec. 2002)
Jones v Commerce Bancorp, Inc, No 06 Civ 835, 2006 WL 1409492 (SDNY, 23 May 2006)
Kapellas v Kofman 459 P2d 912, 922–24 (Cal 1969)
Katz v United States 389 US 347
Kremen v Cohen 337 F 3d 1024 (9th Cir 2003)
Lunney v Prodigy Services Co 683 NYS2d 557, NY App, 2d Div. 1998
Marsha L Shames-Yeakel v Citizens Financial Bank USDC, Northern District of Illinois, Case No. 07-c-5387 (21 August 2009)
Olmstead v United States 277 US 438, 464–65 (1928)
Sanders v ABC 978 P.2d 67, 72 (Cal. 1999)
Scheff v Bock Case No 3022837, Circuit Court, Broward County, Florida
Stratton Oakmont v Prodigy NY Sup Ct 1995
Tucker v Merck & Co 2003 WL 25592785, at *13 (ED Pa 2 May 2003)

Books

1. Adams, Jane and David Birch (eds), *The Digital Identity Reader, 2007* (Mastodon Press, London 2007)
2. Adams, JN, *Character Merchandising* (LexisNexis, UK 1996)
3. Adiga, A, *The White Tiger* (Atlantic Books, London 2008)
4. Agarwala, KN and MD Tiwari, *IT and E-Governance in India* (Macmillan, Michigan 2002)
5. Aggarwal, DD, *Jurisprudence in India Through the Ages* (Kalpaz Publications, New Delhi 2002)
6. Agrawal, KB and V Singh, *Private International Law in India* (KLI, 2010)
7. Akhtar, S and P Arinto (eds), *Digital Review of Asia Pacific 2009-2010* (Sage Publications, Delhi 2007)
8. Anderson, RJ, *Security Engineering: A Guide to Building Dependable Distributed Systems* (Wiley, New York 2001)
9. Anmol Publications, *The Encyclopedia of Hinduism* (Anmol Publications, New Delhi 2000)
10. Atiyah, PS and S Smith, *Introduction to the Law of Contract* (Oxford University Press, Oxford 2006)
11. Badgley, RA *Domain Name* Disputes (Aspen Law & Business Publishers, New York 2002)
12. Bagga, RK, K Keniston and RR Mathur, *The State, IT and Development* (Sage, New Delhi 2005)
13. Balibar, E & I Wallerstein (eds) *Race, Nation, Class: Ambiguous Identities* (Verso, London 1991)
14. Banerjee, SC, *A Brief History of Dharmasastra* (Abhinav Publications, India 1999)
15. Barclay, W, *The Ten Commandments* (Westminster John Knox Press, Louisville 1998)
16. Bartle, RA, *Designing Virtual Worlds* (Pearson Professional Education, NJ 2003)
17. Bauman, Z, *Liquid Modernity* (Polity Press, Cambridge 2000)
18. Baxi, Upendra and Thomas Paul, *Mass Disasters and Multinational Liability: The Bhopal Case* (Indian Law Institute, New Delhi 1986)
19. Bennett, Colin J, *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press, USA 2008)
20. Bennington, Geoff and Brian Massumi (trs), *JF Lyotard: The Postmodern Condition: A Report on Knowledge*, (University of Minnesota Press, Minneapolis 1984)
21. Bezanson, RP, G Cranberg and J Soloski, *Libel Law and the Press: Myth and Reality* (Free Press, NY 1987)
22. Bhansali, SR, *The Information Technology Act 2000: An Exhaustive, Critical and Analytical Commentary of Act No. 21 of 2000* (University Book House, India 2003)
23. Bidgoli, Hossein, *Handbook of Information Security (v. 2): Information Warfare, Social, Legal and International Issues and Security* (John Wiley and Sons Ltd, NY 2006)

24. Biegelman, MT, *Identity Theft Handbook: Detection, Prevention and Security,* (John Wiley and Sons, NJ 2009)
25. Bindloss, Joe, Lindsay Brown, Mark Elliott and Paul Harding, *North East India* (Lonely Planet, Victoria 2007)
26. Birch, DW, *Digital Identity Management: Technological, Business and Social Implications* (Gower Publishing, England 2007)
27. Black, Brian, *The Character of the Self in Ancient India: Priests, Kings, and Women in the Early Upanisads* (State University of New York Press, Albany 2007)
28. Blackstone**,** Sir William, *Commentaries on the Laws of England, Vol I* (Collins, NY 1832)
29. Blamey, Kathleen (tr), *Paul Ricoeur: Oneself as Another* (Chicago University Press, Chicago 1992)
30. Blarkom, GW, J Borking and J Olk, *Handbook of Privacy and Privacy-Enhancing Technologies* (College bescherming persoonsgegevens, The Hague 2003)
31. Bobbio, Norberto, *L'Età dei Diritti* (Einaudi, Torino 1990)
32. Boisson de Chazournes, Laurence and Vera Gowland-Debbas (eds), *The International Legal System in Quest of Equity and Universality,* Liber Amicorum Georges Abi-Saab, (Martinus Nijhoff, Netherlands 2001)
33. Bone, LE, DL Kurtz, *Contemporary Business* (Wiley, 2003)
34. Bone, S (ed), *Osborn's Concise Law Dictionary* (Sweet & Maxwell, 2001)
35. Brands, Stefan A, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy* (The MIT Press, 2000)
36. Brazell, Lorna, *Electronic Signatures Law and Regulation* (Sweet and Maxwell, London 2004)
37. Broom, Herbert, *A Selection of Legal Maxims: Classified and Illustrated* (The Law Book Exchange, NJ 2006)
38. Bygrave, Lee, *Data Protection Law: Approaching Its Rationale, Logic and Limits,* (Kluwer Law International, The Hague 2002)
39. Campbell, Robert (ed), John Austin: *Lectures on Jurisprudence or the Philosophy of Positive Law,* (Law Book Exchange, 2006).
40. Caplan, J & J Torpey (eds), *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton University Press, 2001)
41. Carus, Paul, *Gospel of Buddha* (Kessinger Publishing Co, Kila 2003)
42. Castells, Manuel, M Fernandez-Ardevol, JL Qiu and A Sey, *Mobile Communication and Society: A Global Perspective* (MIT Press, Cambridge 2007)
43. Cates, CL & WV McIntosh, *Law and the Web of Society* (Georgetown University Press, Washington 2001)
44. Cavoukian, Ann and Tyler Hamilton, *The Privacy Payoff: How Successful Businesses Build Consumer Trust* (McGraw Hill, Canada 2002)
45. Cavoukian, Ann, *Privacy by Design… Take the Challenge*, (Jan 2009) <http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf>
46. Cayirci, Erdal and Chunming Rong, *Security in Wireless Ad Hoc and Sensor Networks* (John Wiley and Sons, Chichester 2009)

47. Chakrabarty, Bidyut (ed), *Communal Identity in India: Its Construction and Articulation in the Twentieth Century* (Oxford University Press, New Delhi 2005)
48. Chopra, JK, *Politics of Election Reforms in India* (Mittal Publications, Delhi 1989)
49. Cofta, Piotr, *Trust, Complexity and Control: Confidence in a Converged World* (John Wiley, Chichester 2007)
50. Cohen, A, *Self-Consciousness: An Alternative Anthropology of Identity* (Routledge, London 1994)
51. Corneliussen, HG, JW Rettberg (eds), *Digital Culture, Play, and Identity: A World of Warcraft® Reader* (MIT, USA 2008)
52. Cote, JE & CG Levine, *Identity Formation, Agency and Culture: A Social Psychological Synthesis* (Lawrence Erlbaum Associates, NJ 2002)
53. CSA, *Model Code for the Protection of Personal Information: A National Standard of Canada* (CSA, Etobicoke 1996)
54. Curzon, LB and H Richards, *Longman Dictionary of Law* (Pearson, England 2007)
55. Damer, Bruce, *Avatars! Exploring and Building Virtual Worlds on the Internet* (Peachpit Press, 1998)
56. Danielsen, Dan and Karen Engle (eds), *After Identity: A Reader in Law and Culture* (Routledge, NY 1995)
57. David M Kennedy Center for International Studies, *Culturgrams: Middle East, Asia, Africa, and Pacific Areas* (The Center, 1988)
58. Davis, DR, *The Spirit of Hindu Law* (Cambridge University Press, Cambridge 2010).
59. De Cruz, Peter, *Comparative Law in a Changing World* (Cavendish Publishing London 1999)
60. Deibert, Ronald, JG Palfrey, R Rohozinski, J Zittrain (eds), *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (MIT Press, Cambridge 2010)
61. Derrett, JDM, *Religion, Law and the State in India* (Oxford University Press, Oxford 1999)
62. Desai, TR, *The Indian Contract Act and The Sale of Goods Act* (Lexis Nexis Butterworths Wadhwa, Nagpur 2009).
63. Descartes, René, *Discours de la Méthode* (1861)
64. Detrick, S, *The United Nations Convention on the Rights of the Child: A Guide to the Travaux Preparatoires* (Martinus Nijhoff, Dordrecht 1992)
65. Detrick, Sharon, *A Commentary on the United Nations Convention on the Rights of the Child*, (Martinus Nijhoff, The Hague 1999)
66. Dudley Jenkins, L, *Identity and Identification in India: Defining the Disadvantaged* (Routledge, London 2002)
67. Dumont, Louis, *Essays on Individualism: Modern Ideology in Anthropological Perspective* (University of Chicago Press, Chicago 1986)
68. Dumont, Louis, *From Mandeville to Marx: the Genesis and Triumph of Economic Ideology* (University of Chicago Press, Chicago 1977)
69. Dumont, Louis, *Homo Aequalis* (Galliamard, Paris 1977)
70. Dumont, Louis, *Homo Hierarchicus: The Caste System and its Implications,* (University of Chicago, Chicago 1972)

71. Dunleavy, P and H Margetts, *Government on the Web 2*, *HC 764, Session 2001-2002*, (TSO, 2002)
72. Elliot, Anthony, *Handbook of Identity Studies* (Taylor & Francis, London 2011)
73. English, R and P Havers (QC), *An Introduction to Human Rights and the Common Law* (Hart, Oxford 2000)
74. Fair, Ted, Michael Nordfelt, Sandra Ring and Eric Cole, *Cyberspying: Tracking Your Family's (Sometimes) Secret Online Lives* (Syngress, MA 2005)
75. Feghhi, Jahal, Peter Williams, Jalil Feghhi, *Digital Certificates: Applied Internet Security* (Pearson Education Limited, Harlow 1998)
76. Fertik, Michael, David Thompson, *Wild West 2.0: How to Protect and Restore Your Online Reputation on the Untamed Social* (Amacom, NY 2010)
77. Fischer-Hübner, Simone, Penny Duquenoy, Albin Zuccato and Leonardo Martucci (eds), *The Future of Identity in the Information Society* (Springer, USA 2008)
78. Franck, TM, *The Empowered Self: Law and Society in the Age of Individualism* (Oxford University Press, Oxford 1999)
79. Fuss, Diana *Essentially Speaking: Feminism, Nature and Difference* (Routledge, New York 1989)
80. Gee, JP, *What Video Games Have to Teach Us About Learning and Literacy* (Palgrave Macmillan, NY 2003)
81. Geertz, Clifford, *The Interpretation of Cultures* (Basic Books, New York 1973)
82. Gergen, KJ, *The Saturated Self: Dilemmas of Identity in Contemporary Life* (Basic Books, New York 1991)
83. Glaessner, C, T Kellermann and V McNevin, *Electronic Safety and Soundness: Securing Finance in a New Age* (World Bank, Washington 2004)
84. Glaser, B and A Strauss, *The Discovery of Grounded Theory: Strategies of Qualitative Research* (Wiedenfeld and Nicholson, London 1967)
85. Goffman, Erving, *Stigma: Notes on the Management of Spoiled Identity* (Simon and Schuster, NY 1963)
86. Goffman, Erving, *The Presentation of Self in Everyday Life* (Doubleday, New York 1959)
87. Gokulsing, KM and W Dissanayake, *Indian Popular Cinema: A Narrative of Cultural Change* (Trentham Books, England 2004)
88. Gola, PB, *ICANN: The Introduction of New Top Level Domains (.Info, .Biz, .Name, .Museum, .Aero, .Coop, .Pro) Under the Aspects of Trademark Law And Unfair Competition* (University of California, Los Angeles 2002)
89. Gonzalez-Manet, Enrique, *The Hidden War of Information* (ABC-CLIO, Westport 1989)
90. Gough, Kathleen, *Rural Society in South East India* (Cambridge University Press, UK 1981)
91. Grant, IH (tr), *Jean Baudrillard, Symbolic Exchange and Death* (Sage, London 1993)
92. Grimes, JA, *Ganapati: Song of the Self* (SUNY Press, Albany 1995)
93. Grossfeld, Bernhard, *The Strength and Weakness of Comparative Law* (Clarendon Press, Oxford 1990)

94. Gupta, JND, SK Sharma, MA Rashid, *Handbook of Research on Enterprise Systems* (IGI Global, 2009)
95. Gupta, P and RK Bagga (eds), *Compendium of E-Governance Initiatives in India* (Universities Press, India 2008)
96. Gutman, Amy, *Identity in Democracy* (Princeton University Press, 2003)
97. Hampden-Turner, Charles and Fons Trompenaars, *Riding the Waves of Culture: Understanding Diversity in Global Business* (McGraw-Hill, NY 1997)
98. Harpwood, V, *Modern Tort Law,* (Cavendish Publishing, London 2005)
99. Harpwood, V, *Principles of Tort Law* (Routledge, UK 2000)
100. Hartley, Trevor C *European Union Law in a Global Context: Text, Cases and Material* (Cambridge University Press, Cambridge 2004)
101. Hartmann, Maren, P Rössler and JR Höflich*, After the Mobile Phone? Social Changes and the Development of Mobile Communication* (Frank and Timme, Berlin 2008)
102. Hartney, M (tr), *H Kelsen, General Theory of Norms* (Oxford University Press, Oxford 1991)
103. Hashimoto, Hidetoshi, *The Prospects for a Regional Human Rights Mechanism in East Asia* (Taylor and Francis, London 2003)
104. Hayward, Abraham (tr), Friedrich Karl von Savigny, *Of the Vocation of Our Age for Legislation and Jurisprudence* (Arno Press, New York 1975)
105. Hedley, S, *Tort* (Oxford University Press, Oxford 2006)
106. Hester, JP, *The Ten Commandments: A Handbook of Religious, Social and Legal Issues* (McFarland and Co, North Carolina 2003)
107. Hingorani, AT (ed) *The Gospel of Swadeshi by MK Gandhi* (BVB, Mumbai 1967)
108. HM Government, *A Better Deal for Consumers: Delivering Real Help Now and Change for the Future*, (OPSI, Surrey 2009)
109. Hodgkin, Rachel and Peter Newell, *Implementation Handbook for the Convention on the Rights of the Child* (UNICEF, 2002)
110. Hodgson, Douglas, *Individual Duty Within a Human Rights Discourse* (Ashgate, Aldershot 2003)
111. Hofstede, Geert, *Cultures and Organizations, Software of the Mind: Intercultural Cooperation and its Importance for Survival* (Profile Books, London 1994)
112. Hofstede, Geert, *Culture's Consequences: International Differences in Work-related Values* (Sage, CA 1980)
113. Hogg, MA and J Cooper (eds), *The Sage Handbook of Social Psychology* (Sage, London 2003)
114. Holmes, Stephen and CR Sunstein, *The Cost of Rights: Why Liberty Depends on Taxes* (WW Norton & Co, New York 1999)
115. Horvath, Eniko, *Mandating Identity: Citizenship, Kinship Laws and Plural Nationality in the European Union* (Kluwer Law International, Zuidpoolsingel 2008)
116. Howard, Richard (tr), *Michel Foucault:Madness and Civilization: A History of Insanity in the Age of Reason* (Random House, New York 1965)
117. Hume, David, *A Treatise of Human Nature 1739* (Oxford University Press, Oxford 1978)

118. Huntington, S, *The Clash of Civilizations and the Remaking of World Order* (Simon and Schuster, New York 1996)
119. Hurley, Robert (tr), *Michel Foucault:* The *Use of Pleasure: The History of Sexuality, Vol Two* (Random House, New York 1985)
120. Inwood, Michael, *A Hegel Dictionary* (Blackwell Publishers, Oxford 1992)
121. Islam, Nahid, *The Law of Non-Navigational Uses of International Watercourses* (Wolters Kluwer, Netherlands 2010)
122. Jacobs, A, *The Principal Upanishads: The Essential Philosophical Foundation of Hinduism* (Watkins Publishing, London 2008)
123. James, William, *Principles of Psychology: Vol I* (Henry Holt, New York 1890);
124. Joseph, PT, *Ecommerce: An Indian Perspective* (PHI, India 2006)
125. Kakar, S, *The Inner World: A Psycho-Analytic Study of Childhood and Society in India* (Oxford University Press, Delhi 1981)
126. Kane, PV, *History of Dharmaśāstra Vol 3*, (BORI, Pune 1946)
127. Kane, PV, *History of Dharmasastra: Ancient and Medieval Religious and Civil Law in India Vol 4* (BOR1, Pune 1962-1975).
128. Katz, Jonathan, *Digital Signatures* (Springer, NY 2010)
129. Keniston, Kenneth & Deepak Kumar (eds), *IT Experience in India: Bridging the Digital Divide* (Sage, India 2004)
130. Klever, Alice, *Behavioural Targeting: An Online Analysis for Efficient Media Planning?* (Diplomica Verlag GmbH, Hamburg 2009)
131. Kokswijk, Jacob Van, *Digital Ego: Social and Legal Aspects of Virtual Identity* (Eburon, Eindhoven 2007)
132. Kreitner, Robert *Management* (HMH Publishing, Boston 2006)
133. Krishna Iyer, Justice VR, *The Indian Law: Dynamic Dimensions of the Abstract* (Universal Law Publishing, Delhi 2009)
134. Lamb, GM, *Computers in the Public Service* (Allen and Unwin, Sydney1973)
135. Leary, MR and JP Tangney, (eds), *Handbook of Self and Identity* (Guilford Press, NY 2003)
136. Legrand, Pierre, *Fragments on Law as Culture* (WEJ Tjeenk Willink, 1999)
137. Lessig, L, *Code and Other Laws of Cyberspace* (Basic Books, New York 1999)
138. Lessig, L, *Code: Version 2.0* (Basic Books, New York 2006)
139. Lewis, David, *Convention: A Philosophical Study* (Harvard University Press, MA 1969)
140. Li, Victor H, *Law without Lawyers: A Comparative View of Law in China and the United States* (Westview, 1978).
141. Lingat, Robert, *The Classical Law of India* (University Presses of California, Columbia and Princeton, 1973)
142. Lipschultz, J, *Free Expression in the Age of the Internet: Social and Legal Boundaries* (West View Press, Oxford 2000)
143. Locke, John, *Essay Concerning Human Understanding* (Dent, London 1961)

144. Lyon, David, *Identifying Citizens: ID Cards as Surveillance* (Polity Press, Cambridge 2009)
145. Lyon, David, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge, London 2003)
146. Lyon, David, *Surveillance Studies: An Overview* (Polity Press, US 2007)
147. MacIntyre, A, *Against the Self-Images of the Age* (University of Notre Dame Press, Notre Dame 1978)
148. MacQueen, Hector, Charlotte Waelde, Graeme Laurie, Abbe Brown, *Contemporary Intellectual Property: Law and Policy* (Oxford University Press, Oxford 2010)
149. MacQueen, HL and J Thomson, *Contract Law in Scotland* (Bloomsbury Publishing, Haywards Heath 2007)
150. Maffei, AFX, *English to Konkani Dictionary* (Asian Educational Services, 2007)
151. Mallery, John, J Zann, P Kelly, WJ Noonan, ES Seagren, P Love, R Kraft, M O'Neill, *Hardening Network Security* (McGraw-Hill Education, Europe 2004)
152. Margetts, H *Information Technology in Government: Britain and America* (Taylor and Francis, 1999)
153. Markesinis, BS, Hannes Unberath, *The German Law of Torts: A Comparative Treatise* (Hart, Oregan 2000)
154. Marsh, Jackie, *Popular Culture, New Media and Digital Literacy in Early Childhood* (Routledge, Falmer 2006)
155. Marshall, J, *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights* (Martinus Nijhoff, 2009)
156. Matchett, Freda, *Krsna: Lord or Avatara? The Relationship between Krsna and Vishnu* (Curzon Press, Surrey 2001)
157. Mathur, AD, *Medieval Hindu Law: Historical Evolution and Enlightened Rebellion* (Oxford University Press, Oxford 2007)
158. Mayer, AC, *Caste and Kinship in Central India* (University of California Press, Berkeley 1960)
159. Mayer-Schoenberger, V, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, New Jersey 2009)
160. McBride, NJ, R Bagshaw, *Tort Law* (Pearson Education, Edinburgh 2008)
161. Menski, W, *Comparative Law in a Global Context* (Cambridge University Press, Cambridge 2006)
162. Messner, Wolfgang, *Working with India* (Springer-Verlag Berlin, 2008)
163. Miller, FP, AF Vandome and J McBrewster, *Geotagging* (VDM Publishing House Ltd, Beau Bassin 2009)
164. Miller, PD, *Deuteronomy* (John Knox Press, USA 1990)
165. Mines, Mattison, *Public Faces, Private Voices: Community and Individuality in South India* (University of California Press, California 1994)
166. Mohta, Justice VA, *Trade Marks, Passing Off and Franchising* (All India Reporter, India 2004)

167. Monsma, SV (ed), *Responsible Technology* (WBE Publishing, Michigan 1986)
168. Montesquieu, *Esprit des Lois,* Book I, Chap. 3 (1758)
169. Morgan, Richard and Ruth Boardman, *Data Protection Strategy: Implementing Data Protection Compliance* (Sweet and Maxwell, London 2003)
170. Morsink, Johannes, *The Universal Declaration of Human Rights: Origins, Drafting, and Intent* (University of Pennsylvania Press, Pennsylvania 2000)
171. Murphy, John, *Street on Torts* (Oxford University Press, Oxford 2007)
172. Murroni, C and N Irvine, *Access Matters* (IPPR, London 1998)
173. Narayan, RK, *The Man-Eater of Malgudi* (Penguin, England 1983)
174. Narayanan, P, *Intellectual Property Law* (Eastern Law House, India 2004)
175. Narayanan, P, *Law of Trade Marks and Passing Off* (Eastern Law House, New Delhi 2004)
176. Nardi, Bonnie A and VL O'Day, *Information Ecologies: Using Technology with Heart* (MIT, USA 1999)
177. Nath Dutt, M, *Yajnavalkyasmrti: Sanskrit Text, English Translation, Notes, Introduction and Index of Verses*, (Parimal Publications, New Delhi 2005)
178. Nehru, Jawaharlal, *The Discovery of India* (Signet Press, Calcutta 1946)
179. Oakland, J, *British Civilization: An Introduction,* (Routledge, London 1998)
180. OECD, *OECD Reviews of Regulatory Reform, United Kingdom: Challenges at the Cutting Edge* (OECD, France 2002)
181. Office for National Statistics, *Social Trends 34: National Statistics* (The Stationery Office, London 2004)
182. Office of the Deputy Prime Minister, *English House Condition Survey, 2001: Building the Picture* (ODPM, London 2003)
183. Olivelle, Patrick, *The Dharmasutras: The Law Codes of Ancient India* (Oxford University Press, Oxford 2009)
184. Olson, Carl, *The Many Colours of Hinduism* (Rutgers University Press, NJ 2007)
185. *Oxford Dictionary of Law* (Oxford University Press, Oxford 2009)
186. Paine, Stephen and Mohan Atreya, *Digital Signatures* (McGraw Hill/Osborne, USA 2002).
187. Parrinder, EG, *Avatar and Incarnation* (Oneworld Publications, London 1997)
188. Patrick, Ryan (ed), *Adam Smith: The Theory of Moral Sentiments* (Penguin Books, London 2010)
189. Pellauer, David (tr), *Paul Ricoeur, The Course of Recognition* (Harvard University Press, Harvard 2005)
190. Petronio, Sandra S, *Boundaries of Privacy: Dialectics of Disclosure* (Suny, Albany 2002)

191. Poster, M, *The Mode of Information: Post-Structuralism and Social Context* (Polity Press, Cambridge 1990)
192. Poster, M, *The Second Media Age* (Polity Press, Cambridge 1995)
193. Priban, Jiri, *Legal Symbolism: On Law, Time and European Identity* (Ashgate, Aldershot 2007)
194. PricewaterhouseCoopers and ITGI, *Enterprisewide Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment* (ISACA/ITGI, USA 2003)
195. Pyle, IC & V Illingworth (eds), *The Oxford Dictionary of Computing* (OUP, Oxford 1997)
196. Qian, Yi, D Tipper, P Krishnamurthy, J Joshi, *Information Assurance: Dependability and Security in Networked Systems* (Morgan Kaufmann Publishers, San Francisco 2008)
197. Rajaraman, V, *Essentials of E-Commerce* (PHI, New Delhi 2010)
198. Rama Jois, Justice M, *Legal and Constitutional History of India Vol I* (Universal Law Publishing, India 1984)
199. Rannenberg, Kai, D Royer, A Deuker (eds), *The Future of Identity in the Information Society: Challenges and Opportunities* (Springer, Berlin 2009)
200. Ratanlal, R and KT Dhirajlal, *The Law of Torts* (Wadhwa, Nagpur 2004)
201. Reddy, GB and Mohd Suhaib, *Constitution of India and Professional Ethics* (IKI Publishing, New Delhi 2009)
202. Rheingold, H, *The Virtual Community: Homesteading on the Electronic Frontier* (Addison Wesley, Mass 1993)
203. Rivers, J (tr), R Alexy, *A Theory of Constitutional Rights* (Oxford University Press, Oxford 2002)
204. Rosen, Jeffrey, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage Books, USA 2001)
205. Sabath, AM *International Business Etiquette: Europe* (Career Press, USA 2005)
206. Sahoo, AK, *Sociological Perspectives on Globalisation* (Kalpaz, Delhi 2006)
207. Sankaran Nair, V, *Swadeshi Movement* (Mittal Publishers, Delhi 1985)
208. Schermer, BW, *Software Agents, Surveillance and the Right to Privacy: A Legislative Framework for Agent-enabled Surveillance* (Amsterdam University Press, Amsterdam 2007)
209. Schneider, GP *Electronic Commerce* (Course Technology, Canada 2009)
210. Schroeder, Ralph (ed), *The Social Life of Avatars: Presence and Interaction in Shared Virtual Environments* (Springer, London 2001)
211. Schumann, JH, *The Impact of Culture on Relationship Marketing in International Services:A Target Group-Specific Analysis in the Context of Banking Services* (Deustche Nationalbibliothek, Munchen 2009)
212. Schuyler, Erle, Rich Gibson and Jo Walsh, *Mapping Hacks: Tips and Tools for Electronic Cartography* (O'Reilly Media, CA 2005)

213. Sen, P, *The General Principles of Hindu Jurisprudence* (Saraswat Library, Calcutta 1918)
214. Setalvad, MC, *The Common Law in India* (Hamlyn Trust, 1960)
215. Sharma, A, *Hinduism and Human Rights: A Conceptual Approach* (Oxford University Press, New Delhi 2004)
216. Sharma, JN, *The Political Thought of Lokmanya Bal Gangadhar Tilak* (Concept Publishing, New Delhi 2009)
217. Sharma, SP, *Indian Legal System* (KMR Mittal, Delhi 1991)
218. Sidhpuria, MV, *Retail Franchising* (Tata McGraw Hill: New Delhi 2009)
219. Singh, Sarina, *South India* (Lonely Planet, Victoria 2007)
220. Sinha, Raghuvir, *Dynamics of Change in the Modern Hindu Family* (AKMC, New Delhi 1993)
221. Sinha, RP, *E-Governance in India: Initiatives and Issues* (Centre for Public Policy and Governance, New Delhi 2006)
222. Smith, Gene, *Tagging: People-Powered Metadata for the Social Web* (New Riders, Berkeley 2008)
223. Smith, Graham JH, *Internet Law and Regulation* (Sweet and Maxwell, London 2007)
224. Snell, James, Doug Tidwell and Pavel Kulchenko, *Programming Web Services with SOAP* (O'Reilly, USA 2001)
225. Snyder, JR (tr), Gianni Vattimo, *The End of Modernity: Nihilism and Hermeneutics in Postmodern Culture* (Johns Hopkins University Press, Baltimore 1988)
226. Solbakk, JH, S Holm and B Hofmann, *The Ethics of Research Biobanking* (Springer Verlag, New York 2009)
227. Solove, DJ, M Rotenberg and PM Schwartz, *Privacy, Information and Technology* (Aspen Publishers, New York 2008)
228. Solove, DJ, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York 2006)
229. Solove, DJ, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet* (Yale University Press, Newhaven 2007)
230. Solove, DJ, *Understanding Privacy* (Harvard University Press, Cambridge 2008)
231. Somany, G, *Vishnu and His Avatars,* (Bookwise, India 2004)
232. Sood, Vivek, *Cyberlaw Simplified* (Tata-McGraw Hill, India 2001)
233. Sople, VV, *Managing Intellectual Property: The Strategic Imperative* (Prentice-Hall, New Delhi 2006)
234. Soundarapandian, M, *Literacy Campaign in India* (Discovery Publications, New Delhi 2000)
235. Southwold, Martin, *Buddhism in Life* (Manchester University Press, Manchester 1983)
236. Spivak, GC (tr), *Jacques Derrida of Grammatology* (Johns Hopkins University Press, Baltimore 1974)
237. Stacy, Helen, *Human Rights for the 21st Century: Sovereignty, Civil Society, Culture* (Stanford University Press, Palo Alto 2009)
238. Stengers, Isabelle, *La Vierge et le Neutrino* (Les Empêcheurs de Penser en Rond, Paris 2006)

239. Stone, DL and EF Stone-Romero, *The Influence of Culture on Human Resource Processes and Management* (Lawrence Erlbaum Associates, Mahwah 2007)
240. Stone, J, *The Province and Function of Law: A Study in Jurisprudence* (Harvard University Press, 1946)
241. Stone, Julius, *Social Dimensions of Law and Justice* (Stanford University Press, 1966)
242. Storti, Craig, *Bridging the Communication Gap When Working with Indians* (Intercultural Press, USA 2007)
243. Strawson, PF, *Individuals: An Essay in Descriptive Metaphysics* (Methuen, London 1959)
244. Stryker, S, *Symbolic Interactionism: A Social Structural Version* (Blackburn Press, West Caldwell 2002)
245. Stychin, Carl, *Law's Desire: Sexuality and the Limits Of Justice* (Routledge, London 1995)
246. Sucher, SJ, *The Moral Leader: Challenges, Tools and Insights* (Routledge, US 2007)
247. Sun Microsystems Inc, *Sun Java System Access Manager 7.1 Federation and SAML Administration Guide* (Sun Microsystems, Santa Clara 2007)
248. Sutcliffe, FE (tr), *Rene Descartes, Discourse on Method and Meditations* (Penguin Books, London 1968)
249. Tajfel, H, *Human Groups and Social Categories: Studies in Social Psychology* (Cambridge University Press, Cambridge 1981)
250. Taylor, C, *Philosophy and the Human Sciences: Philosophical Papers 2* (Cambridge University Press, Cambridge 1985)
251. Tazi, Nadia (ed), *Keywords Identity: For a Different Kind of Globalisation* (Other Press, NY 2004)
252. Teece, Geoff, *Hinduism* (Franklin Watts, London 2003)
253. Tomlinson, Hugh (tr), *Nietzsche and Philosophy: Gilles Deleuze* (Columbia University Press, NY 1983)
254. Torremans, Paul, *Hollyoak and Torremans: Intellectual Property Law* (2005)
255. Triandis, HC, *Individualism and Collectivism* (Westview Press, Boulder 1995)
256. Turkle, Sherry, *Life on the Screen: Identity in the Age of the Internet* (Simon & Schuster, New York 1995)
257. Tyler, TR, RM Kramer and OP John (eds), *The Psychology of the Social Self* (Lawrence Erlbaum Associates, NJ 1999)
258. Ullmann-Margalit, Edna, *The Emergence of Norms* (Oxford University Press, Oxford 1977)
259. UNCTAD, *Information Economy Report 2007-2008* (UN, Geneva 2007)
260. Vacca, JR, *Computer and Information Security Handbook* (Elsevier Science & Technology, MA 2009)
261. Vagadia, Bharat, *Outsourcing to India: A Legal Handbook* (Springer, Berlin 2007)

262. Varma, Umeshwar, *Law, Legislature and Judiciary* (Mittal Publications, India 1996)
263. Varma, VP, *Modern Indian Political Thought* (Lakshmi Narain Agarwal, India 1971)
264. Venkataramiah, Justice ES, *Citizenship, Rights and Duties* (BV Naga Publishers, Bangalore 1988)
265. Walker, David M, *The Law of Delict in Scotland* (Sweet & Maxwell, Edinburgh 1981)
266. Walsh, C, *Crime in India,* (Ernest Benn, London 1930)
267. Walters, GJ, *Human Rights in an Information Age: A Philosophical Analysis* (University of Toronto Press, Toronto 2001)
268. Walzer, M, *Spheres of Justice* (Perseus, NY 1984)
269. Warschauer, Mark, *Technology and Social Inclusion:Rethinking the Digital Divide* (MIT Press, 2004)
270. Watson, Alan, *Comparative Law: Law, Reality and Society* (Vandeplas Publishing, FL 2008)
271. Watson, Alan, *Legal Origins and Legal Change* (CIP Group, London1990), 94
272. Watson, Alan, *Legal Transplants: An Approach to Comparative Law,* (Scottish Academic Press, Edinburgh 1974)
273. Watson, Alan, *Society and Legal Change* (Scottish Academic Press, Scotland 1977)
274. Watson, Alan, *The Making of the Civil Law* (Harvard University Press, MA 1981)
275. Weinrib, Ernest J, *The Idea of Private Law* (Harvard University Press, 1995)
276. Wellman, Carl, *A Theory of Rights* (Rowman and Allanheld, NJ 1985)
277. Wellman, Carl, *Real Rights* (Oxford University Press, NY 1995)
278. Wellman, Carl, *The Proliferation of Rights: Moral Progress or Empty Rhetoric?* (Westview Press, Colorado 1999)
279. Westin, AF, *Privacy and Freedom* (Atheneum Press, New York 1967)
280. Windley, PJ, *Digital Identity* (O'Reilly, USA 2005)
281. Woodall, Christopher (tr), *Mario Perniola, Enigmas: The Egyptian Moment in Society and Art* (Verso, London 1995)
282. Wright, D, S Gutwirth, M Friedewald, and Y Punie (eds), *Safeguards in a World of Ambient Intelligence* (Springer, Dordrecht 2010)
283. Yesudian, CAK, *Health Services Utilisation in Urban India: A Study* (Mittal Publications, Delhi 1988)
284. Yin, Robert K, *Applications of Case Study Research* (Sage, Thousand Oaks 2002)
285. Zondervan Publishing, *The Bible:New International Version* (Zondervan Publishing, Grand Rapids 2003)

Book Chapters

1. Aas, K 'Getting Ahead of the Game: Border Technologies and the Changing Space of Governance,' in E Zureik and MB Salter (eds) *Global Surveillance*

and Policing: Borders, Security, Identity (Willan Publishing, Devon 2005), 194-214
2. Berthold, Oliver and Martin Kohntopp, 'Identity Management Based on P3P,' in Hannes Federrath (ed), *Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability* (Springer, Berlin 2001), 141-160
3. Bertino, Elisa and Jason Crampton, 'Security for Distributed Systems: Foundations of Access Control,' in Yi Qian, D Tipper, P Krishnamurthy and J Joshi (eds), *Information Assurance: Dependability and Security in Networked Systems* (Morgan Kaufmann Publishers, San Francisco 2008), 39-80
4. Bharati, Agehananda 'The Self in Hindu Thought and Action,' in AJ Marsella, G DeVos and FL Hsu (eds), *Culture and Self: Asian and Western Perspectives* (Tavistock, London 1985), 185–230
5. Bhargav-Spantzel, A, AC Squicciarini, M Young and E Bertino, 'Privacy Requirements in Identity Management Solutions,' in MJ Smith and G Salvendy (eds) *Human Interface and the Management of Information: Interacting in Information Environments Part II* (Springer, Berlin 2007), 694-702
6. Bhattacharya, DC 'Penances and Vows,' in CPR Aiyar (ed), *Itihasas, Puranas, Dharma and Other Sastras: The Cultural Heritage of India Vol II,* (RMIC, Calcutta 2003), 381-389
7. Birch, David 'Issues and Concerns,' in Jane Adams and David Birch (eds), *The Digital Identity Reader, 2007* (Mastodon Press, London 2007)
8. Birch, DGW 'The Identity Vision,' in DGW Birch (ed), *Digital Identity Management: Perspectives on the Technological, Business and Social Implications* (Gower, Hampshire 2007), 4-5
9. Borbora, S and MK Dutta, 'ICT in Regional Development,' in S Marshall, W Taylor, X Huo Yu (eds), Encyclopedia of Developing Regional Communities with Information and Communication Technology (Idea Group, UK 2006), 387-392
10. Borking, John 'The Use and Value of Privacy-enhancing Technologies,' in Susanne Lace (ed), *The Glass Consumer: Life in a Surveillance Society* (Policy Press, Bristol 2005), 69-98
11. Brewer, MB and M Yuki, 'Culture and Social Identity,' in S Kitayama and D Cohen (eds), *Handbook of Cultural Psychology* (Guilford Publications, New York 2007), 307-322
12. Brown, Ian 'Internet Filtering: Be Careful What You Ask For,' in S Kirca, L Hanson, (eds.), *Freedom and Prejudice: Approaches to Media and Culture* (Bahcesehir University Press, Istanbul 2008), 74-91
13. Brownsword, R 'So What Does the World Need Now? Reflections on Regulating Technologies,' in R Brownsword and K Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oxford 2008), 23-48
14. Bryant, JA and Anna Akerman, 'Finding Mii: Virtual Social Identity and the Young Consumer,' in NT Wood and MR Solomon (eds), *Virtual Social Identity and Consumer Behavior* (ME Sharp Inc, USA 2009)

15. Buchanan, J 'Beyond East and West: Postmodern Democracy in a Mode of Information,' in R Bontekoe & M Stephaniants (eds), *Justice and Democracy: Cross-Cultural Perspectives* (University of Honolulu Press, Honolulu 1997), 423
16. Buldas, Ahto, P Laud and H Lipmaa, 'Accountable Certificate Management Using Undeniable Attestations,' in Pierangela Samarati (ed), *Proceedings of the 7th ACM Conference on Computer and Communications Security* (ACM, New York 2000), 9-17
17. Calvert, SL 'Identity Construction on the Internet' in SL Calvert, AB Jordan and RR Cocking (eds) *Children in the Digital Age: Influences of Electronic Media on Development* (Praeger, Westport 2002), 57-70
18. Camenisch, J and A Lysyanskaya, 'Efficient Non-Transferable Anonymous Multi-Show Credential System With Optional Anonymity Revocation,' in B Pfitzmann (ed), *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology* (Springer Verlag, London 2001), 93–118
19. Camenisch, J and EV Herreweghen, 'Design and Implementation of the *idemix* Anonymous Credential System,' in V Atluri (ed), *Proceedings of the 9th ACM Conference on Computer and Communications Security CCS'02* (ACM Press, NY 2002), 21-30
20. Camenisch, Jan and ors, 'Privacy and Identity Management for Everyone,' in *Proceedings of the Workshop on Digital Identity Management* (ACM, New York 2005), 20-27
21. Carman, John 'Duties and Rights in Hindu Society,' in LS Rouner (ed) *Human Rights and the World's Religions* (University of Notre Dame Press, Notre Dame 1988), 113-128
22. Casassa Mont, M 'Dealing with Privacy Obligations: Important Aspects and Technical Approaches,' in Sokratis Katsikas, J Lopez and G Pernul, *Trust and Privacy in Digital Business*, (Springer, Berlin 2004), 120–131
23. Chavan, AL 'A Dramatic Day in the Life of a Shared Indian Mobile Phone,' in NM Aykin (ed), *Usability and Internationalization: HCI and Culture,* Lecture Notes in Computer Science, 4559/2007, (Springer 2007, New York), 19-26
24. Chen, S, HC Boucher and MW Kraus, 'The Relational Self: Emerging Theory and Evidence,' in VLVignoles, S Schwartz and K Luyckx (eds), *Handbook of Identity Theory and Research* (Springer, New York 2011)
25. Clarke, R and M Wigan,'You are Where You've Been: Location Technologies' Deep Privacy Impact,' in K Michael & MG Michael (eds), *Australia and the New Technologies: Evidence Based Policy in Public Administration* (University of Wollongong, 2008), 100-113
26. Cohn, B 'The Census, Social Structure and Objectification in South Asia,' in B Cohn (ed), *An Anthropologist Among the Historians and Other Essays* (Oxford University Press, Delhi 1987), 224-254
27. Conte, A 'Privacy, Honour and Reputation,' in A Conte, S Davidson and R Burchill (eds), *Defining Civil and Political Rights: The Jurisprudence of the United Nations Human Rights Committee* (Ashgate, Aldershot 2004), 145-160

28. Corrocher, Nicoletta 'The Internet Services Industry: Country Specific Trends in the UK, Italy and Sweden,' in Charles Edquist (ed), *The Internet and Mobile Telecommunications System of Innovation: Developments in Equipment, Access and Content* (Edward Elgar Publishing, Cheltenham 2003), 210-235
29. Cotterrell, Roger 'Seeking Similarity, Appreciating Difference: Comparative Law and Communities,' in E Örücü and A Harding (eds) *Comparative Law in the Twenty-First Century* (Kluwer, The Hague 2002), 35-54
30. Deibert, R N Villeneuve, 'Firewalls and Power: An Overview of Global State Censorship of the Internet,' in M Klang and A Murray (eds), *Human Rights in the Digital Age* (GlassHouse, London 2005), 111-124
31. Deleuze, Gilles, 'Contrôle et Devenir' and 'Post-Scriptum sur les Sociétés de Contrôle' in *Pourparlers 1972–1990* (Minuit, Paris 2003)
32. Duggal, Pavan 'Cyber-crime in India: The Legal Approach,' in Roderic Broadhurst and Peter Grabosky (eds), *Cyber-crime: The Challenge in Asia* (Hong Kong University Press, Hong Kong 2005), 183-196
33. Dumortier, J and C Goemans, 'Privacy Protection and Identity Management,' in B Jerman-Blažič, W Schneider and T Klobučar (eds), *Security and Privacy in Advanced Networking Technologies* (IOS Press, Netherlands 2004), 191-212
34. Edwards, L 'Defamation and the Internet: Name Calling in Cyberspace,' in L Edwards and C Waelde (eds), *Law and the Internet: Regulating Cyberspace* (Hart Publishing, Oxford 1997), 183-198
35. Freeman, Michael 'Counterterrorism and Privacy: The Changing Landscape of Surveillance and Civil Liberties,' in Lee Freeman and Graham Peace (eds), *Information Ethics: Privacy and Intellectual Property* (Information Science Publishing, Hershey 2004), 163-179
36. Freud, S 'The Ego and the Id,' in J Strachey (ed), *The Standard Edition of the Complete Psychological Works of Sigmund Freud (SE) Vol. XIX(1923-1925)* (Hogart Press, London 1974)
37. Friedman, Lawrence 'Some Comments on Cotterrell and Legal Transplants,' in David Nelken and Johannes Feest (eds), *Adapting Legal Cultures* (Hart Publishing, Oxford 2001), 93-99
38. Friedman, Lawrence 'Some Thoughts on Comparative Legal Cultures,' in DS Clark (ed), *Comparative and Private International Law: Essays in Honour of JH Merryman on his Seventieth Birthday* (Duncker and Humblot, Berlin 1990), 49-57
39. Galanter, Marc 'India's Tort Deficit: Sketch for a Historical Portrait,' in DM Engel and M McCann (eds), *Fault Lines* (Stanford University Press, Stanford 2009), 47- 65
40. Gellman, Robert 'A General Survey of Video Surveillance Law in the United States,' in Sjaak Nouwt, BR de Vries and C Prins (eds), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (TMC Asser Press, Netherlands 2005), 7-35
41. Goldschlag, DM, MG Reed and PF Syverson, 'Hiding Routing Information,' in R Anderson (ed), *Information Hiding* (Springer, Berlin 1996), 137-150

42. Gregor, JM and T Gregor, 'Privacy: A Cultural View,' in JR Pennock and JW Chapman (eds), *Privacy Nomos XIII* (Atherton Press, New York 1971), 199-225.
43. Halstead-Nussloch, Richard 'Self-Service, Personalization and Electronic Government,' in Clare-Marie Karat, JO Blom and J Karat (eds), *Designing Personalized User Experiences in E-Commerce* (Springer-Verlag, New York 2004), 161-184
44. Hansen, M 'Marrying Transparency Tools With User-Controlled Identity Management,' in S Fischer-Hubner and ors, (eds), *The Future of Identity in the Information Society*, IFIP 262 (Springer, Boston 2008), 199-220, 202
45. Hanstad, T, RL Prosterman and R Mitchell, 'Poverty, Law and Land Tenure Reform,' in RL Prosterman, R Mitchell, T Hanstad (eds), *One Billion Rising: Law, Land and the Alleviation of Global Poverty* (Leiden University Press, Dordrecht 2009), 17-56
46. Hildebrandt, M 'Profiling and the Identity of the European Citizen' in M Hildebrandt, S Gutwirth (eds), *Profiling the European Citizen: Cross-disciplinary Perspectives* (Springer, Netherlands 2008), 303-344
47. Hsieh, Ann, Todd Hausman and Nerija Titus, 'Influencers and Their Barriers to Technology,' in *Proceedings of the 17th International Conference on World Wide Web* (WWW '08) (ACM, NY 2008), 1103-1104
48. Jayaram, N 'Identity: A Semantic Exploration in India's Society and Culture,' in N Tazi (ed) *Keywords: Identity: For a Different Kind of Globalization* (Sage, Chennai 2004), 125-147
49. Jones, CR 'Nobody Knows You're A Dog: What Amounts to Context in Networked Learning,' in R Land and S Bayne (eds), *Education in Cyberspace* (RoutledgeFalmer, Oxon 2004), 105-116
50. Jøsang, A, J Fabre, B Hay and S Pope, 'Trust Requirements in Identity Management,' in R Buyya and ors (eds) *Proceedings of the 2005 Australasian Workshop on Grid Computing and E-research:Vol 44* (ACS, Australia 2005), 99-108
51. Kelly, Kendall and Jennifer Jones, 'Websites and the Law: An Avenue for Localization,' in Kirk St Amant (ed), *Linguistic and Cultural Online Communication Issues in the Global Age* (IGI Global, Hershey 2007), 202-211
52. Kendall, L 'Recontextualizing 'Cyberspace: Methodological Considerations for On-Line Research,' in S Jones (ed), *Doing Internet Research: Critical Issues and Methods for Examining the Net* (Sage, California 1999), 57-74, 61
53. Konkka, K 'Indian Needs: Cultural End-user Research in Mombai,' in C Lindhom, T Keinonen and H Kiljander, (eds), *Mobile Usability: How Nokia Changed the Face of the Mobile Phone* (McGraw-Hill, New York 2003), 97-112
54. Kuczerawy, Aleksandra 'Facebook and its EU Users: Applicability of the EU Data Protection Law to US based SNS,' in M Bezzi, P Duquenoy, S Fisher-Hubner, M Hansen, G Zhang (eds), *Privacy and Identity,* IFIP AICT 300 (Springer, Germany 2010), 75-85
55. Leenes, Ronald and Isabelle Oomen, 'The Role of Citizens: What Can Dutch, Flemish and English Students Teach Us About Privacy,' in Serge Gutwirth, Y

Poullet, P de Hert, C de Terwangne and S Nouwt (eds), *Reinventing Data Protection* (Springer Verlag, New York 2009), 139-153
56. Leggett, J, G Williams and D Umphress, 'Verification of User Identity via Keyboard Characteristics,' in JM Carey (ed), *Human Factors in Management Information Systems* (Ablex Publishing, NJ 1988), 29-42
57. Legrand, Pierre 'The Same and the Different,' in P Legrand and R Munday (eds) *Comparative Legal Studies: Traditions and Transitions* (Cambridge University Press, Cambridge 2003), 240–311
58. Legrand, Pierre 'What "Legal Transplants?' in David Nelken and Johannes Feest (eds) *Adapting Legal Cultures* (Hart Publishing, UK 2001), 55-68
59. Lessig, Lawrence 'The Laws of Cyberspace,' in Richard A Spinello and Herman T Tavani (eds), *Readings in Cyberethics* (Jones and Bartlett Publishers, Sudbury MA 2004)
60. Lyon, David 'The Border is Everywhere: ID Cards, Surveillance and the Other,' in E Zuriek & MB Salter (eds) *Global Surveillance and Policing: Borders, Security and Identity* (Willan Publishing, Devon 2005), 66-82
61. MacCormick, Neil 'Children's Rights: A Test-Case for Theories of Rights,' in N MacCormick (ed) *Legal Right and Social Democracy: Essays in Legal and Political Philosophy* (Clarendon Press, Oxford 1982), 154-166
62. MacCormick, Neil 'Rights in Legislation,' in PMS Hacker and J Raz (eds), *Law, Morality and Society: Essays in Honour of HLA Hart* (Clarendon Press, Oxford 1977), 189-209
63. MacQueen, HL 'Scots Law' in JM Smits (ed), *Elgar Encyclopaedia of Comparative Law* (Edward Elgar Publishing, Cheltenham 2006), 642-652
64. Manwoo, Lee 'North Korea and the Western Notion of Human Rights,' in JC Hsiung (ed) *Human Rights in East Asia: A Cultural Perspective* (Paragon, New York 1985), 129-151
65. Manzar, O and SS Kazi, '.in India,' in S Akhtar and P Arinto (eds), *Digital Review of Asia Pacific 2009-2010* (Sage, New Delhi 2009), 192-200, 192
66. Marcus, Aaron 'Global and Intercultural User Interface Design,' in JA Jacko and A Sears (eds), *The Human Computer Interaction Handbook* (LEA Publishers, NJ 2003), 441-463
67. Marx, Karl 'On the Jewish Question 1844,' in D McLellan (ed), *Karl Marx: Selected Writings* (Oxford University Press, Oxford 2000), 46-70
68. Messner, Wolfgang, A Hendel, F Thun, 'Rightshore,' in Wolfgang Messner (ed), *Intercultural Aspects of Project Management in India* (Springer, Berlin 2008), 101-120
69. Mutahari, AM 'Primary Principles of Law in Islam,' in OICC, *Islamic Views on Human Rights: Viewpoints of Iranian Scholars* (Alhoda, Tehran 2001), 179-190
70. Myers, Kevin 'English Character and Identity,' in Gary Taylor and Steve Spencer (eds), *Social Identities: Multidisciplinary Approaches* (Routledge, Oxon 2004), 129-144
71. Nabki, Jean-Louis and Martine Ecolasse-Beilecki, 'Variants and Non-variants of Psychological Identity in Employed Females in Different Life Environments,' in Jose Maria Piero, F Prieto, JL Melia, O Luque (eds), *Work and Organisational Psychology: European Contributions of the Nineties* (Taylor and Francis, Hove 1995), 47-60

72. Narayan, Jayaprakash 'Governance: Virtual to Real,' in RK Bagga, K Keniston and RR Mathur (eds), *The State, IT and Development* (Sage, New Delhi 2005), 43-67
73. Nasr, SH 'The Concept and Reality of Freedom in Islam and Islamic Civilization,' in AS Rosenbaum (ed) *The Philosophy of Human Rights* (Greenwood Press, Connecticut 1980), 95-101
74. Nguyen, DT and J Alexander, 'The Coming of Cyberspacetime and the End of Reality,' in R Shields (ed), *Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies* (Sage, London 1996), 99-124
75. Nouwt, Sjaak, BR de Vries and R Loermans, 'Analysis of the Country Reports,' in Sjaak Nouwt, BR de Vries & C Prins (eds), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (TMC Asser Press, The Hague 2005), 323-358
76. O'Hara, Kieron and Nigel Shadbolt, 'Knowledge Technologies and the Semantic Web,' in R Mansell and BS Collins (eds), *Trust and Crime in Information Societies* (Edward Elgar, UK 2007), 113-164
77. Olivelle, P 'Dharmaśāstra: A Literary History,' in T Lubin and D Davis (eds), *Cambridge Handbook of Law and Hinduism* (Cambridge University Press, Cambridge 2010), 28-57
78. Örücü, Esin '*A Project: Comparative Law in Action*,' in E Örücü and D Nelkin (eds), *Comparative Law: A Handbook* (Hart, Oxford 2007), 435-499.
79. Örücü, Esin 'Comparatists and Extraordinary Places,' in Pierre Legrand and Roderick Munday (eds), *Comparative Legal Studies: Traditions and Transitions* (Cambridge University Press, Cambridge 2003), 467-492
80. Perry-Kessaris, Amanda 'Access to Environmental Justice in India's Garden City (Bangalore),' in Andrew Harding (ed), *Access to Environmental Justice: A Comparative Study* (Martinus Nijhoff, Leiden 2007), 59-88
81. Pfitzmann, A, B Pfitzmann and M Waidner, 'ISDN-mixes: Untraceable Communication With Very Small Bandwidth Overhead' in Wolfgang Effelsberg, HW Meuer, and G Müller (eds), *Proceedings of the GI/ITG Conference on Communication in Distributed Systems* (Springer, Germany 1991), 451-463
82. Pfitzmann, A, M Waidner, 'Networks Without User Observability: Design Options,' in F Pichler (ed), *Advances in Cryptology, EUROCRYPT '85: Proceedings of a Workshop on the Theory and Application of Cryptographic Techniques* (Springer, Berlin 1986), 245-253
83. Price, ME and SG Verhulst, 'In Search of the Self: Charting the Course of Self-Regulation on the Internet in a Global Environment,' in CT Marsden (ed), *Regulating the Global Information Society* (Routledge, London 2000), 57-78
84. Prins, Corien 'Property and Privacy: European Perspectives and the Commodification of Our Identity,' in L Guibault and PB Hugenholtz (eds), *The Future of the Public Domain* (Kluwer Law International, The Netherlands 2006), 223–257
85. Raab, C and Bert-Jaap Koops, 'Privacy Actors, Performances and the Future of Privacy Protection,' in Serge Gutwirth, Y Poullet, P de Hert, C de Terwangne and S Nouwt (eds), *Reinventing Data Protection* (Springer, Berlin 2009), 207-225

86. Ramanujam, BK 'Toward Maturity: Problems of Identity Seen in the Indian Clinical Setting,' in S Kakar (ed) *Identity and Adulthood* (Oxford University Press, 1979), 37-55
87. Raz, Joseph 'Rights and Politics,' in J Tasioulas (ed), *Law, Values and Social Practices* (Aldershot, Dartmouth 1997), 75
88. Reed, Drummond and Jerry Kindall, 'Digital Identity,' in Hossein Bidgoli (ed), *The Internet Encyclopedia Volume 1* (John Wiley and Sons Ltd, New York 2004), 493-504
89. Rodrigues, R 'Digital Identity and Anonymity: Desi Manifestations and Regulation,' in S Fischer-Hübner, P Duquenoy, A Zuccato and L Martucci (eds), *The Future of Identity in the Information Society*, IFIP 262 (Springer, Boston 2008), 359–374
90. Rodrigues, R 'User Control Problems and Taking User Empowerment Further,' in V Matyáš, S Fischer-Hubner, D Cvrcek, Petr Svenda (eds), *The Future of Identity*, IFIP AICT 298, (Springer, Germany 2009), 211-225
91. Rouvroy, Antoinette and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy,' in Serge Gutwirth, Y Poullet, P de Hert, C de Terwangne and S Nouwt (eds), *Reinventing Data Protection* (Springer, Berlin 2009), 45-76
92. Rozemuller, Bas 'Chinese Assumed Collectivism Revisited: A Study of the Labor Situation in a Sino-Western Joint Venture,' in Heidi Dahles and Harry Wels (eds), *Culture, Organization and Management in East Asia: Doing Business in China* (Nova Science Publishers, New York 2003), 39-84
93. Savory, RM 'Law and Traditional Society,' in RM Savory (ed) *Introduction to Islamic Civilisation* (Cambridge University Press, Cambridge 1976), 54-60
94. Schafer, Burkhard, Zenon Bankowski, 'Mistaken Identities: The Integrative Force of Private Law' in Mark Van Hoecke and Francois Ost (eds), *The Harmonisation of European Private Law* (Hart Publishing, Oxford 2000), 21-47
95. Scorer, A 'Identity Directories and Databases,' in DGW Birch (ed) *Digital Identity Management: Technological, Business and Social Implications* (Gower, Hampshire 2007), 41-49
96. Seshagiri, Sarita, Sagar Aman and Dhaval Joshi, 'Connecting the "Bottom of the Pyramid": An Exploratory Case Study of India's Rural Communication Environment,' in *Proceedings of the 16th International Conference on the World Wide Web* (ACM Press, New York 2007), 855-862
97. Setalvad, MC 'Culture and Law,' in Raj Kumar (ed) *Essays on Legal Systems in India* (Discovery Publishing House, New Delhi 2003), 73-97
98. Spiekermann, Sarah, Jens Grossklags and Bettina Berendt, 'E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior,' in MP Wellman and Y Shoham (eds), *Proceedings of the 3rd ACM Conference on Electronic Commerce* (ACM, New York 2001), 38-47
99. Stone, A 'Virtual Systems,' in J Crary and SK Winter (eds) *Zone 6: Incorporations* (MIT Press, Mass. 1992), 609-621
100. Stone, AR 'Will the Real Body Please Stand Up? Boundary Stories about Virtual Cultures," in D Bell, BM Kennedy (eds), *The Cybercultures Reader* (Routledge, London 2000), 504-528

101. Van Gelder, Lindsay 'The Strange Case of the Electronic Lover,' in Gary Gumpert and SL Fish (eds), *Talking to Strangers: Mediated Therapeutic Communication* (Ablex, Norwood 1990), 128-142
102. Viola, Francesco 'Personal Identity in the Human Rights Perspective,' in A Peczenik, MM Karlsson (eds), *Law, Justice and the State I: Essays on Justice and Rights* (Franz Steiner Verlag, Stuttgart 1995), 100-109
103. Wheeler, Steve and Helen Keegan, 'Imagined Worlds: Emerging Cultures,' in Steve Wheeler (ed), *Connected Minds, Emerging Cultures: Cybercultures in Online Learning* (Information Age Publishing, USA 2009), 261-276
104. Wilson, G 'Comparative Legal Scholarship' in Michael McConville, Wing Hong Chui(eds), *Research Methods for Law,* (Edinburgh University Press, Edinburgh 2007), 87-103
105. Wiszniewski, Dorian and Richard Coyne, 'Mask and Identity: The Hermeneutics of Self-Construction in the Information Age,' in KA Renninger and Wesley Shumar (eds) *Building Virtual Communities* (Cambridge Press, New York 2002), 191-214
106. Xu, S, R Sandhu and E Bertino, 'TIUPAM: A Framework for Trustworthiness-Centric Information Sharing,' in Elena Ferrari, Ninghui Li, Elisa Bertino and Yuecel Karabulut (eds), *Trust Management III,* IFIP AICT 300 (Springer, Germany 2009), 164-175

Articles, Working Papers, Theses and Conference Papers

1. Abelson, H and L Lessig, 'Digital Identity in Cyberspace,' White Paper submitted for 6.805/Law of Cyberspace: Social Protocols (10 December 1998)
2. Adungo, BI 'Will the Fraud Act 2006 'Get the Law Right?' A Study of the Effectiveness of Applying Criminal Sanctions to Penalise Fraud in the 'Commercial Sphere',' (Masters Thesis, University of Manchester 2007/08)
3. Agarwal, SK 'Content Creation and Dissemination by-and-for Users in Rural Areas' (April 2009) <http://www.researchintouse.com/downloads/spokenweb/VoiKiosk_-_ICTD_09_-_April_09.pdf>
4. Aguiar, Marcos, V Boutenko, D Michael, V Rastogi, A Subramanian and Y Zhou, 'The Internet's New Billion: Digital Consumers in Brazil, Russia, India, China and Indonesia,' BCG Consulting, (September 2010) <http://www.bcg.com/documents/file58645.pdf>
5. Ahmad, Nehaluddin 'Restrictions on Cryptography in India: A Case Study of Encryption and Privacy' (2009) 25 (2) CLSR, 173-180
6. Aizenman Leiner, J '[OpenID] German Court Defines Fundamental Digital Privacy Right,' (15 March 2008) <http://lists.openid.net/pipermail/openid-general/2008-March/013823.html>
7. Aizenman Leiner, J 'Communication to Yadis, IDgang and the VP Symposium' (3 March 2006) <http://lists.danga.com/pipermail/yadis/2006-March/002247.html>

8. Aizenman Leiner, J 'Derecho Ubicuos o Virtuales,' <http:// www.virtualrights.org/ Derechos%20Ubicuos>
9. Aizenman Leiner, J, JM Pedersen and Dr. JM Rivero, 'Virtual Rights: Constituting a Global and Local Information Society,' v.0.9i, (2003), <http://web.archive.org/web/20070221180059/virtualrights.org/files/project_overview_latest.pdf>
10. Akdeniz, Yaman 'Governing Pornography and Child Pornography on the Internet: The UK Approach,' (2001) 32 University of West Los Angeles L Rev, 247-275
11. Akerlof, GA & RE Kranton, 'Economics and Identity,' (2000) 115 Quarterly Journal of Economics, 715
12. Akerlof, GA & RE Kranton, 'Identity and the Economics of Organizations' (2005) 19 Journal of Economic Perspectives, 9
13. Anand, D 'Security Bites: Political Violence and Identity Construction in India,' International Studies Association Annual Conference (Hawaii, March 2005)
14. Andersen, SM, S Chen and R Miranda, 'Significant Others and the Self, (2001) 1 Self & Identity, 159-168.
15. Andrade, NNG de 'Right to Identity: The Foundations for a Renewed Legal Conceptualization,' 3rd International Conference on Computers, Privacy & Data Protection, Brussels (29-30 January 2010).
16. Armitage, CJ and M Conner, The Theory of Planned Behaviour: Assessment of Predictive Validity and Perceived Control,' (1999) 38 Brit J of Soc Psych, 35–54
17. Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of 'Controller' and 'Processor,' Adopted on 16 February 2010, 00264/10/EN, WP 169 <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf>
18. Article 29 Data Protection Working Party, Working Document on On-line Authentication Services, Adopted on 29 January 2003, Brussels, 10054/03/EN, WP 68
19. Aylesworth, Gary 'Postmodernism,' The Stanford Encyclopedia of Philosophy, (2005) <http://plato.stanford.edu/entries/postmodernism/>
20. Bailey, SGM and N Caidi, 'How Much Is Too Little? Privacy and Smart Cards in Hong Kong and Ontario,' (2005) 31 J of Info Sci, 354-364
21. Bainbridge, D 'Criminal Law Tackles Computer Fraud and Misuse,' (2007) 23 (3) CLSR, 276-281
22. Bamford, J 'Identity Management: Achieving Data Protection Compliance and Inspiring Public Confidence,' Position Paper for the Forum on E-Infrastructures for Identity Management and Data Sharing, OII, (2007)
23. Barroso, José Manuel 'Europe: Art or Science,' Speech, Delft University of Technology, (13 January 2006)
24. Bartow, A 'Our Data, Ourselves: Privacy, Propertization, and Gender,' (2000) 34 University of San Francisco LR, 633-704
25. Basu, Ananyo 'Torts in India: Dharmic Resignation, Colonial Subjugation, or "Underdevelopment"?' The South Atlantic Quarterly (Fall 2001), 100 (4), 1053-1070

26. Basu, S and R Jones, 'E-commerce and the Law: A Review of India's Information Technology Act 2000,' (2003) 12 (1) Contemporary South Asia, 7-24
27. Bauer, M, M Meints and Hansen (eds.), 'FIDIS Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems,' Frankfurt a.M., (2005),<http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf>
28. Bechtold, S 'Governance in Namespaces,' (2003) 36 Loyola of LA L Rev, 1248
29. Bénabou, R and J Tirole, 'Identity, Dignity and Taboos: Beliefs as Assets,' IZA Discussion Paper Series (2007), 2583
30. Bennett, CJ 'Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web,' (2001) 3 (3) Ethics and Information Technology, 195-208 <http://www.springerlink.com/content/nj747m13l58450w2/fulltext.pdf>
31. Bhargav-Spantzel, A, J Camenisch, T Gross and D Sommer, 'User Centricity: A Taxonomy and Open Issues,' (2007) 15 (5), J Comp Secur, 493-527
32. Blackman, Josh 'Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet,' (2008) 49 Santa Clara L Rev, 313-392
33. Bodenhorn, H and CS Ruebeck, 'The Economics of Identity and the Endogeneity of Race,' NBER Working Paper Series 9962 (2003)
34. Booth, S and others, 'What are 'Personal Data'? A Study Conducted for the UK Information Commissioner,' (2004) <http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/executive_summary.pdf>
35. Borking, John and Charles Raab, 'Laws, PETs and Other Technologies for Privacy Protection,' 2001 (1) Journal of Information, Law and Technology, <http://elj.warwick.ac.uk/jilt/01-1/borking.html>
36. Bove, M 'Key Management, Setup and Implementation of an Anonymous Credential System,' (Master's Thesis, 2001)
37. Boyd, Clark 'Mapping Censorship,' (2007) 110 (5) Technology Review, 19
38. Boyd, D, M Chang and E Goodman, 'Representations of Digital Identity,' CSCW Workshop (6 November 2004) Chicago <http://people.ischool.berkeley.edu/~dmb/cscw2004-identity/IdentityWorkshopSubmission.pdf>
39. Boyd, danah 'Sexing the Internet: Reflections on the Role of Identification in Online Communities,' Presented at 'Sexualities, Medias, Technologies,' University of Surrey (21-22 June 2001)
40. Brandeis, Louis 'The Right to Privacy,' (1890) 4 Harvard Law Review, 193-220
41. Brands, S 'Secure Access Management: Trends, Drivers and Solutions,' (2002) 7 (3) Information Security Technical Report, 81-94
42. Buell, DA & R Sandhu, 'Identity Management,' (2003) 7 (6) IEEE Internet Computing, 26-28
43. Burgess, JP 'Law and Cultural Identity,' ARENA Working Papers, WP 97/14.

44. Burton Group, 'Primer on Federated Identity,' <http://www.sourceid.org/content/primer.cfm>
45. Cahill, C and ors, 'Liberty Alliance Web Services Framework: A Technical Overview,' Vers.1.0, (14 Feb 2008) <http://www.projectliberty.org/liberty/content/download/4120/27687/file/idwsf-intro-v1.0.pdf>
46. Cai, DA and EL Fink, 'Conflict Style Differences Between Individualists and Collectivists,' (2002) 69 (1) Communication Monographs, 67–87
47. Callero, PL, JA Howard and JA Piliavin, 'Role Identity and Reasoned Action in the Prediction of Repeated Behaviour,' (1987) 50 Soc Psych Q, 247–256
48. Cameron, K 'Microsoft to Adopt Stefan Brands' Technology,' (6 March 2008) <http://www.identityblog.com/?p=934>
49. Cameron, K 'The Laws of Identity,' Microsoft Corporation (2005) <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>
50. Campos Zamora, FJ 'The Emergence of Virtual Entity as Positive Status Information,' <http://www.virtualrights.org/informaci.doc>
51. Cannataci, JA 'Privacy, Technology Law and Religions Across Cultures,' 2009 (1) JILT <http://go.warwick.ac.uk/jilt/2009_1/cannataci>
52. Cantor, S, J Kemp, R Philpott and E Maler (eds), 'OASIS: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0,' OASIS Standard, Security Services Technical Committee (15 March 2005) <http://docs.oasis-open.org/security/saml/v2.0/>
53. Capurro, R 'Privacy: An Intercultural Perspective,' (2005) 7 Ethics and Information Technology, 37-47
54. Carroll-Mayer, M, B Fairweather and BC Stahl, 'CCTV Identity Management and Implications for Criminal Justice: Some Considerations,' (2008) 5 (1) Surveillance and Society, 33-50 <http://www.surveillance-and-society.org/articles5(1)/identity.pdf>
55. Cavoukian, Ann '7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age,' Whitepaper, Information and Privacy Commissioner of Ontario, (2006) <http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf>
56. Cavoukian, Ann 'Privacy in the Clouds, A White Paper on Privacy and Digital Identity: Implications for the Internet' (28 May 2008) <http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf>
57. Cerda, JS 'The Draft Convention on the Rights of the Child: New Rights,' (1990) 12 Human Rights Quarterly, 115-119
58. Cerna, CM 'Universality of Human Rights and Cultural Diversity: Implementation of Human Rights in Different Socio-Cultural Contexts,' (1994) 16 HRQ, 740-752
59. Chansoria, D and R Asoka, 'Digital Signature: Strategic Shift from 'Form' to 'Function',' (2004) 17 CILQ, 269-280
60. Chatterjee, P and S Sarangi, 'Social Identity and Group Lending,' Louisiana State University Departmental Working Papers, 2004-01 (2004)
61. Chaum, David 'Security Without Identification: Transaction Systems to Make Big Brother Obsolete,' (1985) 28 (10) Communications of the ACM, 1030-1044

62. Chaum, David 'Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms,' (1981) 24 (2) Communications of the ACM, 84-90
63. Chinchilla Sandi, Carlos 'Virtual Personality: The Need For Constitutional Reform,' (2005) 082, AR: Revista de Derecho Informático <http://www.alfa-redi.org/rdi-articulo.shtml?x=948>
64. Chittamuru, Deepti 'Millee: Social Dynamics Of Mobile Phone Use By Children In Rural India,' Capstone Project Paper (Spring 2009) <http://www.ischool.berkeley.edu/files/student_projects/MILLEE-_SOCIAL_DYNAMICS_OF_MOBILE_PHONE_USE.pdf>
65. Citron, DK 'Mainstreaming Privacy Torts' (2011) 99 California L Rev, 101-189
66. Clarke, R 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice,' User Identification & Privacy Protection Conference, Stockholm (14-15 June 1999)
67. Clarke, R 'Just Another Piece of Plastic for Your Wallet: The 'Australia Card' Scheme,' (1988) 18 (1) Computers & Society
68. Clarke, R 'Lessons from a Sufficiently Rich Model of (Id)entity, Authentication and Authorisation,' Seminar, University of Toronto, (October 2009) <http://www.rogerclarke.com/ID/IdModel-UT-091026.html>
69. Clarke, R 'The Proposed Australian Implementation of the OECD Privacy Guidelines,' Working Paper (January 1987)
70. Clarke, R 'Why Biometrics Must Be Banned,' Presentation, Baker & McKenzie Cyberspace Law & Policy Centre Conference on 'State Surveillance after September 11, Sydney (8 September 2003) <http://www.rogerclarke.com/DV/Biom030908.html>
71. Cogburn, DL 'Partners or Pawns? Implications for Developing Countries of Elite Decision-Making and Epistemic Communities in Global Information Policy on Developing Countries and Transnational Civil Society,' (2005) 18 (2) Knowledge Technology and Policy, 52-82
72. Coiera, Enrico 'The Impact of Culture on Technology: How Do We Create a Clinical Culture of Innovation?' Editorial, (1999) 171 MJA, 508-509
73. Cole, D 'Artificial Intelligence and Personal Identity,' (1991) 88 (3) Synthese, 399-417
74. Commission of the European Communities, Commission Staff Working Document, Accompanying Document to the Communication From the Commission to the European, Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, Future Networks and the Internet and Early Challenges Regarding the "Internet Of Things" Brussels, 29 September 2008, SEC (2008) 2516
75. Constituent Assembly Debate on the Government of India Act (Amendment) Bill (25 November 1949) <http://indiankanoon.org/doc/1473869/>
76. Crawford, Susan P 'Who's In Charge Of Who I Am? Identity And Law Online,' (2004) 49 NY L Sch L Rev, 211-229
77. Crompton, M 'Proof of ID Required? Getting Identity Management Right,'Australian IT Security Forum (30 March 2004)
78. Dahlberg, L 'The Habermasian Public Sphere Encounters Cyber-Reality,' (2001) 8 (3) The Public, 83-96

79. Dalal, P 'ICT Strategy of India Needs Rejuvenation,' (25 May 2007) <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN029840.pdf>
80. Damania, Farzad 'The Internet: Equalizer of Freedom of Speech? A Discussion on Freedom of Speech on the Internet in the United States and India,' (2002) 12 Ind Intl & Comp L Rev, 243
81. Damiani, E, S De Capitani di Vimercati, P Samarati, 'Managing Multiple and Dependable Identities,' (2003) 7 (6) IEEE Internet Computing, 29–37
82. De Hert, Paul 'Identity Management of e-ID, Privacy and Security in Europe: A Human Rights View,' (2008) 13 (2) Information Security Technical Report, 71-75
83. De Hert, Paul 'Right to Identity to Face the Internet of Things,' (2007) <http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf>
84. De Hert, Paul, W Schreurs and E Brouwer, 'Machine-readable identity documents with biometric data in the EU: Overview of the legal framework,' Keesing Journal of Documents & Identity (2007) 22, 23-26
85. Dean, Roger 'Identity Management: Back to the User,' (2006) 12 Network Security, 4-7
86. Deibert, R, J Palfrey, R Rohozinski and J Zittrain (eds), 'Access Denied: The Practice and Policy of Global Internet Filtering,' (2009) 52 (4) IEEE Transactions on Professional Communication PC, 413-415
87. Dellarocas, C 'The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms,' (2003) 49 (10) Management Science, 1407-1424
88. Department for Constitutional Affairs, 'Increasing Penalties For Deliberate And Wilful Misuse Of Personal Data,' Consultation Paper, CP 9/06 (July 2006) <http://www.dfpni.gov.uk/consultation_misue_of_personal_data.pdf>
89. Department of Information Technology, 'Government Notifications for Enabling e-Services,' <http://mit.gov.in/content/government-notifications-enabling-e-services>
90. Department of Information Technology, 'The National e-Governance Plan,' <http://mit.gov.in/content/national-e-governance-plan>
91. Department of Telecommunications (LR Cell), 'Direction to Block Internet Websites,' No. 820-1/04-LR, Vol-I <http://photos1.blogger.com/blogger/507/157/1600/Indian_censored_list.jpG>
92. Department of Telecommunications (LR Cell), 'Direction to Block Internet Website: Groups.yahoo.com/groups/kynhun,' No. 820-1/2003-LR (Vol I)
93. Desai, Rachana 'Copyright Infringement in the Indian Film Industry,' (2005) 7 Vand J Ent L & Prac, 259-278
94. DH/IPU/Patient Confidentiality, 'NHS Confidentiality Code of Practice,' (November 2003) <http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4069254.pdf>;
95. Dhamija, R and L Dusseault, 'The Seven Flaws of Identity Management: Usability and Security Challenges' (2008) 6 (2) IEEE Security & Privacy, 24-29

96. Diffie, W and ME Hellman, 'New Directions in Cryptography,' (1976) IT-22 (6) IEEE Transactions on Information Theory, 644-654 <http://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf>
97. Donley, C 'Revisiting the Laws of Identity,' Oracle (18 August 2008) <http://blogs.oracle.com/clayton/2008/08/revisiting_the_laws_of_identit.html >
98. Duggal, P 'Cyberlaw in India: The Information Technology Act 2000: Some Perspectives,' (6 September 2001) <http://www.mondaq.com/article.asp?articleid=13430&print=1>
99. Dunleavy, P, H Margetts, S Bastow and J Tinkler, 'New Public Management Is Dead: Long Live Digital-Era Governance,' (2006) 16 (3) J Public Adm Res Theory, 467-494
100. Dyson, Esther 'Digital Identity Management,' Release 1.0, 20 (6) (28 June 2002), 12
101. ECI, 'Handbook for Electoral Registration Officers,' (2008) <http://electionsgoa.nic.in/pdf/handbook_ero.pdf>
102. Economist Intelligence Unit, 'Digital Economy Rankings 2010: Beyond E-readiness,' White Paper, 2010 <http://graphics.eiu.com/upload/EIU_Digital_economy_rankings_2010_FINAL_WEB.pdf>
103. Electoral Commission, 'Can I Search the Electoral Register Online?' <http://www.aboutmyvote.co.uk/faq/registering_to_vote/can_i_search_online.aspx>
104. Erumban, AA, SB Jong, 'Cross-country Differences in ICT Adoption: A Consequence of Culture?' (2006) 41 Journal of World Business, 302–314.
105. European Commission, 'The Economy of Culture in Europe,' Study prepared by the European Commission (October 2006) <http://ec.europa.eu/culture/key-documents/doc873_en.htm>
106. Evans, Katrine 'Hosking v Runting: Balancing Rights in a Privacy Tort,' [2004] PLPR 28
107. Evans, Katrine 'Reverse Gear for NZ's Privacy Tort: The Hosking Decision,' [2003] PLPR 35
108. Everdingen, Y and E Waarts, 'The Effect of National Culture on the Adoption of Innovations,' (2004) 14 (3) Marketing Letters, 217–232
109. Fernandez, DR, DS Carlson, LP Stepina, and JD Nicholson, 'Hofstede's Country Classification 25 Years Later,' (1997) 137 (1) The Journal of Social Psychology, 43-54
110. FIDIS, 'Identity Use Cases & Scenarios,' <http://www.fidis.net/resources/identity-use-cases-scenarios/>
111. Fowle, M 'Interdentity: Belonging, Behaviour and Identity Online,' Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (19-25 February 2006)
112. Francois Paget, 'Identity Theft,' Technical White Paper No 1, (McAfee, 2007)
113. Frankfurt, HG 'Freedom of the Will and the Concept of a Person,' (1971) 68 (1) J of Philosophy, 5-20

114. Friedman, E and P Resnick, 'The Social Cost of Cheap Pseudonyms,' (2001) 10 (1) J Eco and Mgt Strategy, 173-199
115. Galanter, Marc 'Legal Torpor: Why So Little Has Happened in India After the Bhopal Tragedy,' (1985) 20 Texas Intl LJ, 273-294
116. Galanter, Marc 'The Displacement of Traditional Law in Modern India' (1968) 24 (4) J of Soc Iss, 65-91
117. Gandy, O 'The Surveillance Society: Information Technology and Bureaucratic Social Control,'(1989) 39 (3) Journal of Communication, 61-76
118. Gaspay, A, S Dardan and L Legorreta, 'Software of the Mind: A Review of Applications of Hofstede's Theory to IT Research,'(2007) 9 (3) Journal of Information Technology Theory and Application <http://aisel.aisnet.org/jitta/vol9/iss3/3>
119. Gasser, Urs 'Identity 2.0: Privacy as Code and Policy' (9 February 2006) <http://blogs.law.harvard.edu/ugasser/2006/02/09/identity-20-privacy-as-code-and-policy/>
120. Gasser, Urs, JG Palfrey, 'Case Study: Digital Identity Interoperability and eInnovation,' Berkman Center Research Publication No. 2007-11, <http://cyber.law.harvard.edu/interop/pdfs/interop-digital-id.pdf>
121. Gavison, Ruth 'Privacy and the Limits of Law,' (1980) 89 (3) The Yale Law Journal, 421-471
122. Gewirth, Alan 'Are There Any Absolute Rights?' (1981) 31 (122) The Philosophical Quarterly, 1-16
123. Giordano, Philip 'Invoking Law as a Basis for Cyberspace,' 1998 Stan Tech L Rev 1
124. GMC, 'Confidentiality, Guidance for Doctors,' (12 October 2009) <http://www.gmc-uk.org/static/documents/content/Confidentiality_core_2009.pdf>
125. Goldschlag, DM, MG Reed, 'Onion Routing For Anonymous and Private Internet Connections,' (1999) 42 (2) Communications of the ACM, 84–88.
126. Goodstein, L 'Do American Theories Apply Abroad: American Business Values and Cultural Imperialism,' Commentary, (Summer1981), Organizational Dynamics, 49-54
127. Graham, S and D Wood, 'Digitizing Surveillance: Categorization, Space, Inequality,' (2003) 23 (2) Critical Social Policy, 227-48
128. Great Britain Parliament House of Lords Select Committee on the Constitution, 'Surveillance: Citizens and the State,' 2nd Report of Session 2008-09, Vol. 2, Evidence, House of Lords papers 18-II (2008-09)
129. Greenleaf, GW and J Nolan, 'The Deceptive History of the Australia Card' (1986) 58 (4) Aust Qtly, 407-425
130. Greenwood, D 'The Context for Identity Management Architectures and Trust Models,' Proceedings of the OECD Workshop on Digital Identity Management, Norway (2007)
131. Gritzalis, Stefanos 'Privacy Issues in the Digital Era,' Guest Editorial, (2006) 16 (2) Internet Research, 117
132. Gross, B 'Information Sharing Within and Outwith the NHS,' CSAGS Secretariat, (30 November 2000)

<http://www.csags.scot.nhs.uk/Meeting%20Papers/CSAGS%202000-03.PDF>
133. Guarda, P and N Zannone, 'Towards the Development of Privacy-Aware Systems,' (2009) 2 Information and Software Technology, 337-350
134. Guha, S 'The Politics of Identity and Enumeration in India c. 1600–1990,' (2003) 45 (1) Comp Studies in Soc and Hist, 148-167
135. Gutwirth, Serge 'Beyond Identity?' (2009) 1 (1) IDIS, 123-133 <http://www.springerlink.com/content/j4396418218787pm/fulltext.pdf>
136. Haga, SB and LM Beskow, 'Ethical, Legal and Social Implications of Biobanks for Genetics Research,' (2008) 60 Advances in Genetics, 505-544;
137. Handford, PR 'Moral Damage in Germany,' ICLQ (1978) 27, 849-875
138. Hansard HC 'Offences Against Children: Internet,' col 692W (2 November 2009)
139. Hansard HL, Debate on Identity Cards Bill, cols 46-53 (21 March 2005)
140. Harrison, J and P Bramhall, 'New Approaches to Identity Management and Privacy: A Guide Prepared for the Information Commissioner,' (December 2007) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/edentity_hp_idm_paper_for_web.pdf>
141. Hart, HLA 'Are There any Natural Rights?' (1955) 64 Philosophical Review, 175-191
142. Heisenberg, D and M-H Fandel, 'Projecting EU Regimes Abroad: The EU Data Protection Directive as Global Standard,' Paper presented at the Annual Meeting of the American Political Science Association, Boston, Massachusetts (28 August 2002) <http://www.allacademic.com/meta/p65517_index.html>
143. Hillman, Robert A and JJ Rachlinski, 'Standard-Form Contracting in the Electronic Age,' (2002) 77 NYUL L Rev, 429
144. Hodgson, D 'The International Legal Protection of the Child's Right to a Legal Identity and the Problem of Statelessness,' (1993) 7 (2) Intl J L and Family, 255-270
145. Home Office (IPS), 'National Identity Service Cost Report: October 2009,' Presented to Parliament Pursuant to Section 37 of the Identity Cards Act 2006, <http://www.ips.gov.uk/cps/files/ips/live/assets/documents/IPS_Cost_report_2009_v5.pdf>
146. Home Office (IPS), 'Why Do We Need the National Identity Scheme?' <http://www.ips.gov.uk/identity/scheme-why.asp>.
147. Hsu, Carol, R Davison and S Stares, 'Cultural Influences on Attitudes Towards Hong Kong's Smart Identity Card,' PACIS 2004 Proceedings, (2004) <http://aisel.aisnet.org/pacis2004/20>
148. Hunt, J 'Do American Theories Apply Abroad: Applying American Behavioural Science, Some Cross Cultural Problems,' (Summer 1981) Organizational Dynamics, 55-62
149. IBM Research, 'IDEMIX (Identity mixing)'<http://www.zurich.ibm.com/pri/projects/idemix.html>

150. ICM Research, 'Personal Information Survey,' (February 2008) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/icm_research_into_personal_information_feb08.pdf>
151. ICO, 'Data Protection Technical Guidance: Determining What is Personal Data,' (2007), <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf>
152. ICO, 'Key Definitions of the Data Protection Act,' <http://www.ico.gov.uk/for_organisations/data_protection_guide/key_definitions_of_the_dpa.aspx>
153. ICO, 'Privacy Enhancing Technologies (PETs),' Data Protection Technical Guidance Note, (2006) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies.pdf>
154. ICO, 'The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection,' (March 2010) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_dividend.pdf>
155. ICO, 'Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998' (May 2002) <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/health_data_-_use_and_disclosure001.pdf>
156. ICPP, ULD and SNG, 'Identity Management Systems (IMS): Identification and Comparison Study,' (September 2003) <https://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf>
157. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, 'Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information' (6 June 1995) <http://aspe.hhs.gov/datacncl/niiprivp.htm>
158. Jean Camp, L 'Digital Identity,' (2004) 23 (3) IEEE Technology and Society Magazine, 34-41
159. Jean Camp, L 'Identity in Digital Government,' Report of the Digital Government Civic Scenario Workshop, (2003), 29 <http://www.ljean.com/files/identity.pdf>
160. Jensen, Robert 'The Digital Provide: Information (Technology), Market Performance and Welfare in the South Indian Fisheries Sector,' (2007) 122 (3) Q J Econ, 879-924
161. Johnson, M and KM Rogers, 'The Fraud Act 2006: The E-Crime Prosecutor's Champion or the Creator of a New Inchoate Offence?' (2007) 21 (3) Intl Rev of Law, Computers and Technology, 295-304
162. Jøsang, Audun, D Povey and A Ho, 'What You See is Not Always What You Sign,' Proceedings of the Australian Unix User Group Symposium, Melbourne (September 2002) <http://persons.unik.no/josang/papers/JPH2002-AUUG.pdf>
163. Joseph, CA and AP Kavoori, 'Mediated Resistance: Tourism and the Host Community,' (2001) 28 (4) Annals of Tourism Research, 998-1009

164. Karas, S 'Privacy, Identity, Databases,' (2002) 52 Am U L Rev, 394-445
165. Karnow, CEA 'The Encrypted Self: Fleshing out the rights of Electronic Personalities,' (1994) 13 JCIL 1
166. Kendall, L 'Meaning and Identity in "Cyberspace": The Performance of Gender, Class, and Race Online,' (1998) 21 Symbolic Interaction, 129-53.
167. Kirby, MD 'Transborder Data Flows and the "Basic Rules" of Data Privacy,'(1980)16 Stan J Intl L, 27-66
168. Kirschenbaum, MG 'Why I Blog Under My Own Name (and a Modest Proposal),' (9 July 2005) <http://www.otal.umd.edu/~mgk/blog/archives/000813.html>
169. Kishwar, M 'Who Am I? Living Identities vs. Acquired Ones,' Revised Version of Keynote Address, UNHCR and AIW Conference on 'Women in Search of Identity,' March 1996 <http://www.infinityfoundation.com/mandala/s_es/s_es_kishw_who_frameset.htm>
170. Kohl, J and B Clifford Neuman, 'The Kerberos Network Authentication Service (Version 5),' Internet Request for Comments RFC-1510, (Sept 1993)
171. Koops, Bert-Jaap and ors, 'A Typology of Identity-Related Crime,' (2009) 12 (1) Communication & Society, 11- 24
172. Koops, BJ and RE Leenes, 'ID theft, ID fraud and/or ID-related Crime: Definitions Matter,' (2006) 30 (9) Datenschutz und Datensicherheit, 553-556
173. Korff, D 'Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons,' (February 2001) <http://europa.eu.int/comm/internal_market/privacy/studies/legal_en.htm>
174. Kormann, DP and AD Rubin, 'Risks of the Passport Single Signon Protocol,' (2000) 33 Computer Networks, 51–58
175. Kumaraguru, P and L Cranor, 'Privacy in India: Attitudes and Awareness,' Proceedings of the 2005 Workshop on Privacy Enhancing Technologies, Dubrovnik (30 May - 1 June 2005) <http://www.cs.cmu.edu/~ponguru/PET_2005.pdf>
176. Kumaraguru, P, L Cranor and E Newton, 'Privacy Perceptions in India and the United States: An Interview Study,' 33rd Research Conference on Communication, Information and Internet Policy, The National Center for Technology and Law, George Mason University School of Law, USA, (23 - 25 September 2005)
177. Kutner, Luis 'Legal Philosophers: Savigny: German Lawgiver,' (1972) 55 Marq L Rev, 280-296
178. Laudon, KC 'Markets and Privacy,' (1996) 39 Communications of the ACM, 93
179. Lee, Tahirih V 'Risky Business: Courts, Culture and the Marketplace,' (1993) 47 U Miami L Rev, 1335-1414
180. Leenes, RE 'User-Centric Identity Management As An Indispensable Tool For Privacy Protection,' (2008) 2 (4) IJIPM, 345-371

181. Leenes, Ronald, J Schallaböck and M Hansen (eds), 'Privacy and Identity Management for Europe,' PRIME Whitepaper, Ver. 2, (June 2007) <www.prime-project.eu/ prime_products/whitepaper>
182. Legrand, Pierre 'Against a European Civil Code,' (1997) 60 MLR 44-63 (**1997a**)
183. Legrand, Pierre 'The Impossibility of "Legal Transplants,"'(1997) 4 Maastricht J Eur & Comp L. 111-124 (**1997b**)
184. Legrand, Pierre 'European Legal Systems Are Not Converging,' (1996) 45 ICLQ 52 - 81
185. Legrand, Pierre 'How to Compare Now' (1995) 16 LS 232
186. Legrand, Pierre 'On the Singularity of Law,' (2006) 47 Harv Intl LJ 517-530
187. Lemley, Mark 'Terms of Use,' (2006) 91 Minn L Rev 459
188. Liberty Alliance Project, Liberty Alliance Project Whitepaper: Personal Identity (23 March 2006) <www.projectliberty.org/liberty/content/download/395/2744/file/Personal_Identity.pdf>
189. Lidsky, LB 'Prying, Spying and Lying: Intrusive Newsgathering and What the Law Should Do About It,' (1998) 73 Tul L Rev, 173-248
190. Litman, J 'Information Privacy/Information Property,' (2000) 52 Stanford Law Review, 1283-1313
191. Loncke, M 'Identity: A Legal Perspective,' FIDIS WP2 Workshop, 2-3 December 2003
192. Lord Bingham, 'The Way We Live Now: Human Rights in the New Millennium,' (1999) 1 Web JCLI
193. Luft, Joseph and Harry Ingham, 'The Johari Window, A Graphic Model of Interpersonal Awareness,' Proceedings of the Western Training Laboratory in Group Development, UCLA, LA (1955)
194. Lyon, David 'Biometrics, Identification and Surveillance,' (2008) 22 (9) Bioethics, 499-508
195. Lyon, David 'Identity Cards: Social Sorting by Database,' OII Internet Issue Brief No. 3 (2004) <http://www.oii.ox.ac.uk/research/publications.cfm>
196. MacQueen, HL 'Searching for Privacy in a Mixed Jurisdiction,' (2006) 21 Tulane European and Civil Law Forum, 73
197. Madelin, J and L Razzell, 'Towards an Identity Society,' White Paper, <http://www.identitysociety.org/files/identitysociety.pdf>
198. Madhava Prasad, M 'The State and Culture: Hindi Cinema in the Passive Revolution' (PhD thesis, University of Pittsburgh 1994)
199. Mahapatra, Prasanta and ors, 'Civil Registration Systems and Vital Statistics: Successes and Missed Opportunities,' (29 October 2007) <https://www.who.int/healthinfo/statistics/WhoCounts2.pdf>
200. Maler, E and D Reed, 'The Venn of Identity: Options and Issues in Federated Identity Management,' (2008) 6 (2) Security and Privacy: IEEE in Security & Privacy, 16-23
201. Margetts, Helen 'E-Government in Britain: A Decade On,' (2006) 59 (2) Parliamentary Affairs, 250-265

202. Markesinis, B 'Privacy, Freedom of Expression and the Horizontal Effect of the Human Rights Bill: Lessons From Germany,Wilberforce Lecture 1998, LQR (1999) 115, 45-88
203. Marshall, BA and ors, 'Social Networking Websites in India and the United States: A Cross-National Comparison of Online Privacy And Communication' (2008) 9 (2) Iss in Info Systems, 87-94
204. McAlpine, Mhairi 'E-portfolios and Digital Identity: Some Issues for Discussion,'(2005) 2(4), E-Learning and Digital Media, 378-387
205. Meijer, EM and R Ling, 'The Adoption and Use of ICT Services in Europe: Potential Acceptance of Mobile Broadband Services,' EURESCOM P903 (2006) <www.eurescom.de/~ftproot/web-deliverables/public/P900-series/P903/ICT_use_ ante.pdf>
206. Melissaris, E 'The More The Merrier? A New Take on Legal Pluralism,'(2004) 13 (1) Soc Leg Studies, 57-79
207. Menyhart, Russell 'Changing Identities and Changing Law: Possibilities for a Global Legal Culture,' (2003) 10 (2) Indiana Journal of Global Legal Studies, 157-199
208. Michael Froomkin, A 'The Essential Role of Trusted Third Parties in Electronic Commerce,' (1996) 75 Ore L Rev 49
209. Miller, B 'Vital Signs of Identity,' (1994) 31 (2) IEEE Spectrum, 22-30
210. Ministry of Communication and Information Technology (DIT), 'Order: Blocking of Websites,' 7 July 2003, New Delhi, Gazette of India, GSR 529(E), Extra, Pt II
211. Ministry of Human Resource Development Government of India, 'Study on Copyright Piracy in India,' (1999) Ch VIII
212. Mistry, Pranav 'The Thrilling Potential of SixthSense Technology,' TEDIndia Mysore, India (2009) <http://www.pranavmistry.com/projects/sixthsense/>
213. Mitra, Kana 'Human Rights in Hinduism,'(1982) 19 J Ecu Studies 77
214. Mordini, E and S Massari, 'Body, Biometrics and Identity,' (2008) 22 (9) Bioethics, 488-498
215. Mowbray, M 'Implementing Pseudonymity' (2006) 3 (1) SCRIPTed 34 <http://www.law.ed.ac.uk/ahrc/script-ed/vol3-1/mowbray.asp>
216. Nabeth, T 'Privacy in the Context of Digital Social Environments: A Cyber-Sociological Perspective,' INSEAD CALT-FIDIS Working Paper, (2005)
217. Nagral, A 'Privacy in Public Hospitals' (1995) 3 (1) Indian Journal of Medical Ethics
218. National Commission to Review the Working of the Constitution, 'Liability of the State in Tort,' Consultation Paper (2001)
219. Norberg, P, DR Horne and DA Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviours,' (2007) 41 (1) J Cons Aff, 100-126
220. Noveck, BS 'Trademark Law and the Social Construction of Trust: Creating the Legal Framework for On-Line Identity,' (2003) 83 Wash ULQ 1733

221. Oakley, Kate 'What is E-Governance,' Resource Paper, (Council of Europe, 2003)
222. OECD, 'At a Crossroads: "Personhood" and Digital Identity in the Information Society,' STI Working Paper, 2007/7, Information and Communication Technologies, DSTI/DOC (2007) 7.
223. Okita, C '(Digital) Identity 2.0' (October 2007) <http://www.usenix.com/publications/login/2007-10/pdfs/okita.pdf>
224. Olsen, T and T Mahler, 'Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust' Part II,' (2007) 23 CLSR, 415-426
225. Oppliger, R 'Microsoft .NET Passport and Identity Management,' (2004) 9 (1) Information Security Technical Report, 26-34
226. Oram, Andy 'The Long View of Identity,' O'Reilly (29 June 2006) <http://onlamp.com/pub/a/onlamp/2006/06/29/the-long-view-of-identity.html?page=1>
227. Oram, Andy 'What Sociologist Erving Goffman Could Tell Us About Social Networking and Internet Identity,' O'Reilly Radar (26 October 2009) <http://radar.oreilly.com/2009/10/what-sociologist-erving-goffma.html>
228. Pande, Rekha 'Digital Bridge or Digital Divide: Assessing Gender Equations and the Indian Experience in Information and Communication Technologies,' Paper Presented at the Annual Meeting of the International Studies Association, Montreal, Canada (17 March 2004)
229. Panikkar, R 'Is the Notion of Human Rights a Western Concept? A Hindu/Jain/Buddhist Reflection,' (1982) 30 Diogenes, 75-102
230. Paulos, E and E Goodman, 'The Familiar Stranger: Anxiety, Comfort and Play in Public Places,' Proceedings of the Conference on Human Factors and Computing Systems, CHI 2004, Vienna (24-29 April 2004)
231. Peek, Marcy 'The Observer and the Observed: Re-imagining Privacy Dichotomies in Information Privacy Law,' (2009) 8 (1) Nw J Tech & Intell Prop, 51-66
232. Peerenboom, RP 'What's Wrong With Chinese Rights? Towards a Theory of Rights with Chinese Characteristics,'(1993) 29 (6) Harv Hum Rts J, 39-47
233. Pei, Cao 'The Origins of Mediation in Traditional China,' 54 Disp Res J (1999) 32
234. Pentland, A, R Fletcher and A Hasson, 'Dak Net: Rethinking Connectivity in Developing Nations,' IEEE Computer Society, (January 2004), 78 – 83
235. Pfitzmann, A and M Hansen, 'Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management: A Consolidated Proposal for Terminology,' v0.31 (15 February 2008) <http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf>
236. Phelps, Joseph Glen Nowak and Elizabeth Ferrell, 'Privacy Concerns and Consumer Willingness to Provide Personal Information,'(2000) 19 J Pub Policy & Mktg, 27-41

237. Phillipson, Gavin 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act,' (2003) 66 MLR, 726-728
238. Pollock, Sir George 'Report on the Indian Penal Code' (1850) 13, The Calcutta Review, 171
239. Post, RC 'Three Concepts of Privacy' (2001) 89 Geo LJ, 2087
240. PRIME Advanced Tutorial, Vers. 3 (May 2008) <http://blues.inf.tu-dresden.de/prime/Tutorial_V2/DevTut.html>
241. PRIME General Public Tutorial, Vers. 2 (May 2008) <http://blues.inf.tu-dresden.de/prime/GPTv2/englisch/PRIME_nm.htm>
242. PRIME General Public Tutorial, Vers. 2 (May 2008) <http://blues.inf.tu-dresden.de/prime/GPTv2/englisch/PRIME_nm.htm>
243. Prins, JEJ 'Een Recht op Identiteit,' (2007) 82 (14) Nederlands Juristenblad, 849
244. Raab, C 'Keynote Address,' Proceedings of the Life of Mobile Data, University of Surrey, Guildford (April 2004)
245. Radetzki, Marcus 'From Communism to Capitalism in Laos: The Legal Dimension,' (1994) 34 (9) Asian Survey, 799-806
246. Radhakrishnan, S 'The Hindu Dharma,' (1922) 33 (1) Intl J Ethics, 1-22
247. Raju, Dr KD 'WTO-TRIPS Obligations and Patent Amendments in India: A Critical Stocktaking' (2004) 9 JIPR, 242-259
248. Ramamurthy, R 'Data Theft and Identity Theft: A Review,' ITU Telecom World Geneva (5-9 October 2009) <http://www.itu.int/tlc/WORLD2009/forum/entries/participant.148030.html>
249. Ramanathan, R 'Globalisation, Values and Democracy,' (February 2004) <http://www.indiatogether.org/2004/feb/opi-values.htm>
250. Rapaport, WJ 'Computer Processes and Virtual Persons: Comments on Cole's "Artificial Intelligence and Personal Identity," Technical Report 90-13 (Buffalo Dept. of Computer Science, May 1990)
251. Raz, Joseph 'Legal Rights,' (1984) 4 OJLS, 1-21
252. Raz, Joseph 'The Nature of Rights,' (1984) 93 Mind, 194-214
253. Reich, CA 'The Individual Sector,' (1991) 100 (5) Yale L J, 1409-1448
254. Resnick, P, R Zeckhauser, E Friedman and K Kuwabara, 'Reputation Systems,' (2000) 43 (12) Communications of the ACM, 45-48
255. Rewa, Jessica 'The True Public Sphere of India: Withstanding the Threats of Globalization and Consumerism,' (2007) <http://drcdev.ohiolink.edu/bitstream/handle/123456789/3631/JessicaRewa2007.pdf?sequence=1>
256. Riley, Chris, K Buckner, G Johnson and D Benyon, 'Culture & Biometrics: Regional Differences in the Perception of Biometric Authentication Technologies,' (2009) 24 (3) AI & Soc, 295-306
257. Rivest, RL, A Shamir and L Adleman, 'A Method For Obtaining Digital Signatures and Public-Key Cryptosystems,' (1978) 21 (2) Communications of the ACM, 120–126
258. Roberts, G and ors, 'Reflective Learning, Future Thinking: Digital Repositories, E-portfolios, Informal Learning and Ubiquitous Computing,'

White Paper, (2005) <http://www.alt.ac.uk/docs/ALT_SURF_ILTA_white_paper_2005.pdf>
259. Roberts, K and N Boyacigiller, 'Cross-national Organizational Research: The Grasp of the Blind Men,' (1984) 6 Research in Organizational Behaviour, 423-475
260. Rodrik, D 'World Too Complex for One-Size-Fits-All Models,' (2007) 44 Post-Autistic Economics Review, 73-74 <http://www.paecon.net/PAEReview/issue44/Rodrik44.pdf>
261. Rogerson, Simon 'The Virtual World: A Tension between Global Reach and Local Sensitivity,' (2004) 2 (11/2004) Intl J of Information Ethics, 1-7
262. Rosenthal, M'What was Postmodernism,' (1992) 22 (3) Soc Rev, 83-105
263. Roussos, G, D Peterson and U Patel, 'Mobile Identity Management: An Enacted View,' (2003) 8 Intl J Elec Commerce, 81-100
264. RSA Labs, 'Public-Key Cryptography Standards (PKCS),' Chapter 2, <http://www.rsa.com/rsalabs/node.asp?id=2165>
265. Rundle, Mary and B Laurie, 'Identity Management as a Cybersecurity Case Study,' OII Conference on Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities, Research Publication No 2006-01, (2005) <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2006_01_Rundle_IdentityManagement_CybersecurityCaseStudy.pdf>
266. Salim, N 'Breach of Privacy and Confidentiality Under Information Technology Act, 2000' Legal Service India (10 January 2009) <http://www.legalserviceindia.com/article/l288-Breach-of-privacy-&-Confidentiality-.html>
267. Sandel, Michael J 'The Procedural Republic and the Unencumbered Self,' Political Theory (Feb 1984) 12 (1), 81-96
268. Sastri, TVG 'General Concept of *Maya* and its Applications,' Journal of the Oriental Institute, (1975) 24, 343-356
269. Schau, HJ & MC Gilly, 'We Are What We Post? Self-Presentation in Personal Web Space,' (2003) 30 (3) J Cons Res, 385-414
270. Schwartz, Paul M 'European Data Protection Law and Restrictions on International Data Flows,'(1995) 80 Iowa Law Review, 471-496
271. Schwartz, Paul M 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States,' (1995) 80 Iowa Law Review, 553- 618
272. Sellar, WDH 'Scots Law: Mixed From the Very Beginning? A Tale of Two Receptions,' (2000) 4 EdinLR 3
273. Senicar, Vanja, Borka Jerman-Blazic and Tomaz Klobucar, 'Privacy-Enhancing Technologies: Approaches and Development,' (2003) 25 (2) Computer Standards & Interfaces, 147-158
274. Shah, N 'Subject to Technology: Internet Pornography, Cyber-Terrorism and the Indian State,' (2007) 8 (3) Inter-Asia Cultural Studies, 349 - 366
275. Simon, SJ 'The Impact of Culture and Gender on Websites: An Empirical Study,' (2000) 32 (1) SIGMIS Database, 18-37

276. Smith II, Dr Earl R 'Can't We Simplify Digital Identity,' Guest Article, The Federal Circle (26 August 2010)
277. Smith, D 'The Challenge of Federated Identity Management,' (2008) 4 Network Security, 7-9
278. Smith, Seagrumn 'Microsoft and the European Union Face Off Over Internet Privacy Concerns,' (2002), Duke L & Tech Rev 0014
279. Soenens, Els 'Mobile Identity and Location Based Services,' in WP11, D11.4: Workshop on Mobility and Identity, 20 April 2006 <http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp11-del11.4.workshop_on_MIDM.pdf>
280. Sokefeld, M 'Debating Self, Identity and Culture in Anthropology,' (1999) 40 (4) Current Anthropology, 417-447
281. Sommer, D, M Casassa Mont, S Pearson, 'PRIME Architecture V3,' Deliverable D14.2.d, (9 July 2008), <https://www.prime-project.eu/prime_products/reports/arch/pub_del_D14.2.d_ec_WP14.2_v3_Final.pdf>
282. Sommer, P, 'Identity Management Systems: The Forensic Dimensions,' The 18th Annual FIRST Conference, Seville (June 2007) <http://www.first.org/conference/2007/papers/sommer-peter-slides.pdf>
283. Sproull, Lee and Sara Kiesler, 'Reducing Social Context Cues: Electronic Mail in Organizational Communication,' (1986) 32 Management Science, 1492-1512
284. Stalder, Felix 'The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy,' (2002) 7 (2) Sociological Research Online <http://www.socresonline.org.uk/7/2/stalder.html>
285. Stryker, S 'Identity Salience and Role Performance: The Importance of Symbolic Interaction Theory for Family Research,' (1968) 30 J Marriage and the Family, 558–564
286. Sucharitkul, Sompong 'Thai Law and Buddhist Law,' (1998) 46 Am J Comp L, 69-72
287. Sullivan, Clare 'Digital Identity: An Emergent Legal Concept: An Analysis of the Role and Legal Nature of Digital Identity in a Transactional Context' (PhD thesis, University of Adelaide 2009)
288. Sullivan, Clare 'Privacy or Identity?' (2008) 2 (3) IJIPM, 289-324
289. Summers, B 'The Fraud Act 2006: Has it Had Any Impact?' (2008) 75 Amicus Curiae <http://sas-space.sas.ac.uk/dspace/bitstream/10065/1783/1/amicus75_summers.pdf.pdf>
290. Swami Krishnananda, The Mundaka Upanishad, (Divine Life Society, Sivananda Ashram) <http://www.sankaracharya.org/library/mundaka.pdf>
291. Swidler, A 'Culture in Action: Symbols and Strategies,'(1986) 51 American Sociological Review, 273-286
292. Teubner, Gunther 'Legal Irritants: Good Faith in British Law or How Unifying Law Ends up in New Differences,'(1998) 61 (1) MLR 11-32
293. The Gallup Organisation, Data Protection in the EU: Data Controllers' Perceptions (EC Flash Barometer No 226), Brussels (17 April 2008) <http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf>

294. Torrubia, A, FJ Mora, L Marti, 'Cryptography Regulations for E-commerce and Digital Rights Management,' (2001) 20 (8) Computers & Security, 724-738
295. Triandis, HC, R Bontempo, MJ Villareal, M Asai, N Lucca, 'Individualism and Collectivism: Cross-cultural Perspectives on Self-ingroup Relationships,' (1988) 54 (2) Journal of Personality and Social Psychology, 323-338
296. Turkle, S 'Computational Technologies and Images of the Self,' (1997) 64 (3) Social Research, 1094-1111
297. UIDAI, 'Creating a Unique Id for Every Resident in India,' Working Paper, vers 1.1 <http://uidai.gov.in/documents/Creating_a_unique_identity_for_every_resident_in_India.pdf>
298. UK Information Commissioner, 'The "Durant" Case and its Impact on the Interpretation of the Data Protection Act 1998,' (27 February 2006) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf>
299. Umphress, D and G Williams, 'Identity Verification Through Keyboard Characteristics,' (1965) 2 (1) Int J Man-Machine Studies, 263-273.
300. UNESCO, 'Code of Ethics for the Information Society,' (2007) <http://portal.unesco.org/ci/en/files/24935/11841676611Code_of_Ethics.pdf/Code%2Bof%2BEthics.pdf>
301. UNICEF, 'Civil Rights Commentary,' <http://www.unicef.org/pon98/06-13.pdf>
302. US Department of Commerce, 'Privacy and the NII: Safeguarding Telecommunications-Related Personal Information,' (October 1995) <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>
303. Vasalou, A and AN Joinson, 'Me, Myself and I: The Role of Interactional Context on Self-Presentation Through Avatars,' (2009) 25 (2), Computers and Human Behaviour, 510-520
304. Veeraragavan, B 'Torts In India Whether Unnecessary Or Simply Overlooked,' LegalService India (6 December 2007)
305. Walker, Katherine 'It's Difficult to Hide It": The Presentation of Self on Internet Home Pages,' (2000) 23 (1) Qualitative Sociology, 99-120
306. Wang, M 'Electronic Signatures,' (2007) 23 (1) CLSR, 32-41
307. Wang, WenJie, Yufei Yuan, Norm Archer, 'A Contextual Framework for Combating Identity Theft,' (2006) 4 (2) IEEE Security & Privacy, 30-38
308. Waskul, D and M Douglas, 'Cyberself: The Emergence of the Self in On-line Chat,' (1997) 13(4) The Information Society, 375-397
309. Watson, Alan 'Comparative Law and Legal Change,'(1978) 37 CLJ, 313-336
310. Watson, Alan 'Legal Transplants and European Private Law,' (2000) 44 (2) EJCL <http://www.ejcl.org/ejcl/44/44-2.html>
311. Watson, Alan 'Legal Transplants and Law Reform' (1976) 92 LQR, 79-84
312. Whitman, JQ 'The Two Western Cultures of Privacy: Dignity Versus Liberty," (2004) 113 Yale Law Journal 1151

313. Williams, Katie ‘Space Per Person in the UK: A Review of Densities, Trends, Experiences and Optimum Levels,’ Review, (2009), 26S Land Use Policy, S83–S92
314. Willison, S ‘How to Use OpenId,’ (22 December 2006), <http://www.youtube.com/watch?v=Vq0R1Y1A2rE&feature=player_embedded>
315. Wilton, R ‘Racingsnake, The Blog of Future Identity: Is Privacy only for the Rich?’ Blogpost (11 March 2009)
316. Wilton, Robin ‘What’s the Value of Your Digital Identity,’ Keynote Address, OTS 2010, Maribor (June 2010) <http://www.futureidentity.eu/documents/RW-Maribor.pdf>
317. Wood, P ‘Implementing Identity Management Security: An Ethical Hacker's View,’ (2005) 9 Network Security, 12-15
318. WP 37 of the Article 29 Working Party, ‘Privacy on the Internet - An Integrated EU Approach to On-line Data Protection,’ (November 2000) <http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2000/wpdocs00_en.htm>
319. Zhao, S, S Grasmuck and J Martin, ‘Identity Construction on Facebook: Digital Empowerment in Anchored Relationships,’ (2008) 24 (5), Computers in Human Behavior, 1816-1836
320. Zimmerman, DL ‘Requiem for a Heavyweight: A Farewell to Warren and Brandeis’s Privacy Tort,’ (1983) 68 Cornell L Rev, 291-367
321. Zittrain, Jonathan ‘Be Careful What You Ask For: Reconciling a Global Internet and Local Law,’ The Berkman Centre for Internet & Society, Harvard Law School Research Publication No. 2003-03, 5/2003 <http://cyber.law.harvard.edu/home/uploads/204/2003-03.pdf>

Reports

1. Bhargav-Spantzel, Abhilasha, AC Squicciarini and E Bertino, ‘Establishing and Protecting Digital Identity in Federation Systems,’ CERIAS Tech Report 2007-18 <https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2007-18.pdf>
2. Booz, Allen and Hamilton, ‘Achieving Universal Access,’ A Report for the Prime Minister's Policy Unit (2000)
3. BT, ‘Security Report: Online Identity Theft,’ February 2006 <http://www.btplc.com/onlineidtheft/onlineidtheft.pdf>
4. Budde.Com, ‘India - Internet Market,’ Report, (05 July 2010) <http://www.budde.com.au/Research/India-Internet-Market.html>
5. CIFAS, ‘Fraud Trends,’ 2006-2010, <http://www.cifas.org.uk/default.asp?edit_id=562-57>
6. CIFAS, ‘The Anonymous Attacker: A Special Report on Identity Fraud and Account Takeover,’ (2009) <http://www.cifas.org.uk/download/The_Anonymous_Attacker_CIFAS_Special_Report.pdf>
7. Commission of the European Communities, ‘First Report on the Implementation of the Data Protection Directive,’ COM (2003) 265 (01), (15

May 2003)
<http://eurlex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf>
8. Communication by the Italian Privacy Commissioner in House of Commons Canada, 'A National Identity Card for Canada?' Report of the Standing Committee on Citizenship and Immigration (October 2003) <http://oipc.bc.ca/pdfs/public/cimmrp06-e.pdf>
9. CRID (University of Namur), First Analysis of the Personal Data protection Law in India, Report delivered in the Framework of Contract JLS/C4/2005/15 between CRID and the Directorate General Justice, Freedom and Security <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf>
10. Cser, A, Jonathan Penn, 'Identity Management Market Forecast: 2007 To 2014: Provisioning Will Extend its Dominance of Market Revenues,' Forrester Research (6 February 2008) <http://www.forrester.com/Research/Document/Excerpt/0,7211,43842,00.html>
11. Department for Culture, Media and Sport and Department for Business, Innovation and Skills, 'Digital Britain,' Final Report, Presented to Parliament by the Secretary of State for Culture, Media and Sport and the Minister for Communications, Technology and Broadcasting (June 2009)
12. G8, 'Digital Opportunities for All: Meeting the Challenge: Report of the Digital Opportunity Task Force (DOT Force) Including a Proposal for a Genoa Plan of Action,' (May 2001) <http://www.dotforce.org/reports/>
13. Great Britain Parliament House of Commons Home Affairs Committee, 'A Surveillance Society?' 5th Report of Session 2007-08, Vol 2, Oral and Written Evidence, House of Commons Papers 58-II 2007-08, (TSO)
14. Great Britain Parliament House of Lords Science and Technology Committee, 'Personal Internet Security,' 5th Report of Session 2006-07, Vol 2 Evidence, HL papers 165-II 2006-07 (TSO)
15. House of Commons Science and Technology Committee, 'Identity Card Technologies: Scientific Advice, Risk and Evidence,' HC 1032, Sixth Report of Session 2005-06 (TSO: UK 2006); Home Office, 'Legislation on Identity Cards: A Consultation,' CM 6178 (TSO, UK 2004)
16. IAMAI & IMRB, 'Internet in India,' Report, (2007) <http://www.iamai.in/Upload/Research/I-Cube-2007-Summary-Report-final.pdf>
17. IAMAI, 'Mobile Internet in India,' Report (December 2009) <http://www.iamai.in/Upload/Research/MobileInternetinIndia_39.pdf>;
18. IAMAI, 'Report on Mobile VAS in India,' (July 2010) <http://www.iamai.in/Upload/Research/Report_on_MVAS_(2010)_submittal_42.pdf>
19. IMRB and IAMAI, 'Internet in India: 2006,' Summary Report (6 December 2006) <http://www.iamai.in/Upload/Research/book.pdf >
20. ITU, 'Internet Report 2006, 'Digital.Life,' (December 2006) <http://www.itu.int/osg/spu/publications/digitalife/docs/digital-life-web.pdf>

21. ITU, 'Internet Reports 2005: The Internet of Things,' (2005) <http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf>
22. Jain, Rekha 'The Telecoms Sector: India Infrastructure Report 2001,' <http://www.iitk.ac.in/3inetwork/html/reports/IIR2001/iir8.pdf>
23. Joyce, R and G Gupta, 'User Authentication Based on Keystroke Latencies' Technical Report 5, Department of Computer Science, James Cook University, Australia (1969)
24. Kable, 'Identity Management in the UK Public Sector to 2011,' Research Report (July 2007)
25. Miller, David L Carey and MM Combe, 'The Boundaries of Property Rights in Scots Law,' Report to the XVIIth International Congress of Comparative Law (2006)10 (3) EJCL <www.ejcl.org/103/art103-4.doc>
26. Miller, Eric 'Wireless Internet Access in Rural South India' (December 2000) <http://ccat.sas.upenn.edu/~emiller/report.html>
27. NHS Information Authority, The Consumers' Association and Health Which, 'Share with Care: People's Views on Consent *and* Confidentiality of Patient Information,' Final Report (October 2002) <http:<//www.connectingforhealth.nhs.uk/resources/archive/share_with_care.pdf>
28. Norton Online Living Report 2009 <http://www.nortononlineliving.com/documents/NOLR_Report_09.pdf>
29. Parliament of India, Rajya Sabha, Department-Related Parliamentary Standing Committee on Home Affairs, 'One Hundred and Sixteenth Report on the State Emblem of India (Prohibition of Improper Use) Bill 2004,' (25 August 2005)
30. Pato, J 'Identity Management: Setting Context,' Encyclopedia of Cryptography and Security, (Summer/Fall 2003) <http://www.hpl.hp.com/techreports/2003/HPL-2003-72.pdf>
31. RNCOS, 'Global RFID Market Analysis till 2010,' Strategic Report, (August 2010)
32. The Privacy Protection Study Commission, 'Personal Privacy in an Information Society,' Report (July 1977) <http://epic.org/privacy/ppsc1977report/>
33. UIDAI, 'Aadhaar-Communicating to a Billion: An Awareness and Communication Report,' ACSAC (17 May 2010) <http://uid-india.com/Documents/AADHAAR_CommPDF.pdf>
34. US Department of Health, Education and Welfare, 'Records, Computers and the Rights of Citizens,' (1973)
35. US Federal Trade Commission, 'Identity Theft Survey Report,' 7 (2003)
36. WorldBank, Development Indicators, <http://data.worldbank.org/indicator/IT.CMP.PCMP.P2>

News Articles

1. ABH News, 'Foursquare Roads to 3 Million Users,' *ABH News* (31 August 2010) <http://abh-news.com/foursquare-roads-to-3-million-users-4049.html>

2. Azamgarh, MF ‘Plight of the Living Dead,’ *TimeAsia,* (19 July 1999) <http://www.time.com/time/asia/asia/magazine/1999/990719/souls1.html>
3. BBC News, ‘UK Consumers Enjoy 'Advanced' Digital Communications’ *BBC News* (17 December 2009) <http://news.bbc.co.uk/1/hi/8417521.stm>
4. Becker, D ‘Passport to Nowhere?’ *CNET News.com* (23 March 2004) <http://news.cnet.com/Passport-to-nowhere/2100-7345_3-5177192.html>
5. Blair, Tony ‘Tony Blair’s Full Speech,’ *The Guardian* (7 March 2000) <http://www.guardian.co.uk/uk/2000/mar/07/tonyblair>
6. Blakely, R ‘When Prison is Just a Phone Call Away’ *The Times* (6 April 2009)
7. Brian, Matt ‘Is UK Public WIFI Doomed?’ *The Next Web* (28 February 2010) <http://thenextweb.com/uk/2010/02/28/uk-public-wifi-doomed/>
8. Chatterjee, MB ‘Nine Submit Bids for UID Tender,’ *The Hindu Business Line* (21 June 2010) <http://www.thehindubusinessline.com/2010/06/22/stories/2010062251760800.htm>
9. Clark, A ‘Oracle's takeover of Sun Microsystems comes as surprise to software industry,’ *The Guardian* (20 April 2009) <http://www.guardian.co.uk/business/2009/apr/20/sun-microsystems-oracle-takeover>
10. Costa, D ‘Identity Crisis,’ *PC Magazine* (15 October 2002) <http://www.pcmag.com/print_article2/0,1217,a=31229,00.asp>
11. Dikshit, S ‘Bid to Block Anti-India Website Affects Users,’ *The Hindu* (23 September 2003) <http://www.thehindu.com/2003/09/23/stories/2003092312761100.htm>
12. Dixit, P ‘Social Networkers: A New Generation,’ *Hindustan Times* (14 January 2011)
13. Economist Intelligence Unit, Digital Identity Authentication in E-commerce, *The Economist* (March 2007) <http://graphics.eiu.com/ebf/PDFs/IdenTrust_digital_authentication_Web_PDF_final.pdf>
14. Express News Service, ‘Computerised Chart Display System Arrives at Vadodara Railway Station’ (23 February 2009) <http://www.expressindia.com/latest-news/computerised-chart-display-system-arrives-at-vadodara-railway-station/426910/>
15. Fildes, Jonathan ‘India’s Vision for a Digital Billion,’ *BBC News* (6 February 2007) <http://news.bbc.co.uk/1/hi/technology/6322027.stm>
16. Fonseca, Brian ‘New Identity Management Products Abound,’ *Infoworld* (20 June 2003) <http://www.infoworld.com/d/security-central/new-identity-management-products-abound-793>
17. FTC, ‘Microsoft Settles FTC Charges Alleging False Security and Privacy Promises’ (8 Aug 2002) <http://www.ftc.gov/opa/2002/08/microsoft.shtm>
18. Ganapati, Priya ‘Mumbai Police Gag Hinduunity.org,’ (May 2004) <http://us.rediff.com/news/2004/may/26hindu.htm>
19. Hartley, M ‘Facebook to Tweak its Privacy, Security Policies to Meet Canadian Law,’ *Financial Post* (17 August 2009) <http://www.financialpost.com/news-sectors/technology/story.html?id=1901523>

20. Higham, Nick 'Privacy Law Remains Confused,' *BBC News* (9 June 2003) <http://news.bbc.co.uk/1/hi/uk/2975718.stm>
21. Indo-Asian News Service, 'Charges Framed Against Student For Threat Mail to Kalam,' *MSN News* (3 September 2009) <http://news.in.msn.com/national/article.aspx?cp-documentid=3202934>
22. Infosecurity, 'Access and Authentication Market: Ready to Meet Tomorrow's Critical Needs?' techFocus, *InfoSecurity* (January 2009) <http://fanaticmedia.com/infosecurity/archive/Jan%2009/Authentication%20Market.htm>
23. Jena, C 'It's All About Identity,' *Express Computer* (19 February 2007) <http://www.expresscomputeronline.com/20070219/market02.shtml>
24. Joseph, J 'How The UID Project Can Be A Cause For Concern,' *CNN-IBN* (5 October 2010) <http://ibnlive.in.com/news/how-the-uid-project-can-be-a-cause-for-concern/132375-3.html>
25. Lassaussois, Jacques 'Procès Clinton : Où va la Justice Américaine? *Gazette du Palais* (18-19 March 1998)
26. Le Monde, 'Le Recours à l'Intimité est de Règle aux Etats-Unis, *Le Monde* (22 April 2002)
27. Lemos, Robert 'Password Flaw Cracks Passport Security,' *CNET News.com* (8 May 2003) <http://news.cnet.com/2100-1002_3-1000429.html>
28. Leyden, John 'German Wi-Fi Networks Liable for 3rd Party Piracy,' *The Register* (13 May 2010) <http://www.theregister.co.uk/2010/05/13/open_wifi_fines_germany/>
29. Mahapatra, Dhananjay 'Bloggers Can be Nailed for Views,' *Times of India* (24 February 2009) <http://timesofindia.indiatimes.com/India/Bloggers-can-be-nailed-for-slur/articleshow/4178823.cms>
30. Merinews, 'Haryana Publishes Entire Voters Lists With Photo' *Merinews* (3 March 2009) <http://www.merinews.com/article/haryana-publishes-entire-voters-lists-with-photo/15712414.shtml>
31. Meyer, D 'Pub 'Fined £8k' for Wi-Fi Copyright Infringement,' *ZDNet UK* (27 November 2009) <http://news.zdnet.co.uk/communications/0,1000000085,39909136,00.htm>
32. Meyer, David 'Open Wi-Fi 'Outlawed' by Digital Economy Bill,' *ZDNet UK* (26 February 2010) <http://www.zdnet.co.uk/news/networking/2010/02/26/open-wi-fi-outlawed-by-digital-economy-bill-40057470/>
33. Natu, Nitasha 'Tuff Shoes Case: Madhu, Milind Plead Not Guilty,' *Times of India* (29 October 2004) <http://timesofindia.indiatimes.com/articleshow/903786.cms>
34. Nelson, Dean 'Romantic' Darjeeling Bans Public Displays of Affection,' *Telegraph News* (7 September 2009) <http://www.telegraph.co.uk/news/worldnews/asia/india/6146863/Romantic-Darjeeling-bans-public-displays-of-affection.html>
35. Out-Law News, 'Business Rival Makes Highest Ever Online Libel Payout,' *Out-LAW News* (3 April 2008) <http://www.out-law.com/page-9011>
36. Out-Law News, 'US Sex offenders to Be Banned from Social Networking for the First Time' *Out-LAW News* (13 February 2008) <http://www.out-law.com/page-8870>

37. Pathak, Rujul 'No Public Display of Affection Please, We Are Indian!' *Times of India* (5 June 2003) <http://timesofindia.indiatimes.com/Ahmedabad-Events/No-public-display-of-affection-please-we-are-Indian/articleshow/45961507.cms#ixzz0zhQ209g5>
38. Prakash, Nivedan 'Building a Holistic Security Approach,' *Express Computer* (29 March 2010) <http://www.expresscomputeronline.com/20100329/20thanniversary07.shtml>
39. Press Information Bureau, 'Approval for Introducing the National Identification Authority of India Bill 2010 in Parliament' (24 September 2010) <http://pib.nic.in/newsite/pmreleases.aspx?mincode=61>
40. Pt, Sebastian 'The Card Trick,' 3 (9) *Outlook Business* (20 April-3 May 2008)
41. PTI, 'Orkut Forum on Shivaji Maharaj Blocked,' *ExpressIndia* (18 November 2006) <http://www.expressindia.com/fullstory.php?newsid=77287>
42. Reuters, 'EU: MS Passport Is Under Investigation' *ZDNet News* (2002) <http://zdnet.com.com/2100-1104-934916.html>
43. Robertson, Brian 'Indian ID Market Geared for Growth,' (2005) 17 (2) *Card Technology Today*, 11
44. Sahu, S and R Guha, 'India Wants to See Google, Skype Data,' *The Wall Street Journal* (2 September 2010)
45. SC Staff, 'Claims Made that the Digital Economy Bill Will Cause the End of Public WiFi,' *SC Magazine* (23 March 2010) <http://www.scmagazineuk.com/claims-made-that-the-digital-economy-bill-will-cause-the-end-of-public-wifi-as-open-rights-group-plans-demonstration-tomorrow/article/166316/>
46. Sharma, S 'Crisis for Identity or Identity Crisis?' *D-sector.org* (12 October 2010) <http://www.d-sector.org/article-det.asp?id=1396>
47. Slemko, M 'Microsoft Passport to Trouble,' (5 November 2001) <http://www.znep.com/~marcs/passport/>
48. Sparkes, M 'Europeans Value Personal Data as Highly as Cash,' (12 October 2007) <http://www.macuser.co.uk/news/129476/europeans-value-personal-data-as-highly-as-cash.html>
49. Sreekala, G 'Much Hyped IT Act stays a Dead Letter,' *Times News Network* (20 July 2006) <http://economictimes.indiatimes.com/News/Business_Law/General_Law/Much_hyped_IT_Act_stays_a_dead_letter/articleshow/1783026.cms>
50. Steiner, P *The New Yorker* (5 July 1993) 69 (20)
51. Telegraph.co.uk, 'Law Student Wins £10,000 After Being Branded a Paedophile on Facebook,' (28 July 2010) <http://www.telegraph.co.uk/technology/facebook/7912731/Law-student-wins-10000-after-being-branded-a-paedophile-on-Facebook.html>
52. Thakur, Atul '33% of Indians Live in Less Space than US Prisoners,' *The Economic Times* (25 November 2008) <http://economictimes.indiatimes.com/News/PoliticsNation/33-of-Indians-live-in-less-space-than-US-prisoners/articleshow/3754519.cms>
53. The Associated Press, 'Gere Kiss Leads to Legal Complaints in India,' *USA Today* (18 May 2007) <http://www.usatoday.com/life/people/2007-04-16-gere-kiss_N.htm>

54. The Economist, 'The Next Billion Geeks: How the Mobile Internet Will Transform the BRICI Countries,' *The Economist* (2 September 2010), <http://www.economist.com/node/16944020?story_id=16944020&fsrc=rss>
55. The New Yorker, 'On the Internet, Nobody Knows You're a Dog,' *The New Yorker,* 69 (20) (1993) <http://www.unc.edu/depts/jomc/academics/dri/idog.html>
56. The Telegraph, 'India Gives BlackBerry More Time,' *The Telegraph* (31 Aug 2010) <http://www.telegraph.co.uk/technology/blackberry/7972926/India-gives-BlackBerry-more-time.html>
57. Vyas, R 'Perfect Semblance: Imperfect Law,' *The Telegraph* (9 January 2009) <http://www.telegraphindia.com/1090109/jsp/opinion/story_10356023.jsp>

Websites

1. Anonymizer <http://www.anonymizer.com/>
2. AOL Terms of Use <http://about.aol.com/aolnetwork/aolcom_terms>
3. Bebo <http://s.bebo.com/>
4. CA Technologies <http://www3.ca.com/Solutions/ProductFamily.asp?ID=4839>
5. CACI YOIS (Youth Offending Information System) <http://www.socialsoftware.co.uk/Development/172.asp>
6. Captcha <http://www.captcha.net/>
7. ClaimId <http://claimid.com/>
8. Credentica <http://www.credentica.com/u-prove_sdk.html>
9. Eclipse <http://www.eclipse.org/higgins/>
10. EMC (RSA) <http://www.rsa.com/>
11. EPIC <http://www.epic.ca>
12. European Parliament <http://www.europarl.europa.eu>
13. Express Computer Online <http://www.expresscomputeronline.com>
14. Facebook <www.facebook.com>
15. FIDIS Deliverables <http://www.fidis.net/resources/fidis-deliverables/>
16. FIDIS <http://www.fidis.net/>
17. Friendster <www.friendster.com>
18. Garlik <http://www.garlik.com/>
19. Google <www.google.com>
20. Guardian <http://www.guardian.co.uk>
21. Hi5 <http://hi5.com/ >
22. HP <www.hp.com>
23. IBM <http://www.ibm.com/>
24. ICANN <http://www.icann.org/>
25. Identity Commons <http://wiki.idcommons.net/Identity_Commons>
26. Identity Gang <http://identitygang.org/>
27. Info Security <http://infosecuritymag.techtarget.com/2002/apr/cover_casestudy.shtml>
28. Information Commissioner's Office (UK) <www.ico.gov.uk>

29. Internet Watch Foundation <http://www.iwf.org.uk/>
30. Internet2 <http://www.Internet2.edu>
31. ITU Focus Group on Identity Management <http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html>
32. ITU Identity Management Global Standards Initiative <http://www.itu.int/ITU-T/gsi/idm/>
33. ITU Joint Coordination Activity for Identity Management <http://www.itu.int/ITU-T/jca/idm/>
34. Kim Cameron's Identity Weblog <http://www.identityblog.com/stories/2004/12/09/thelaws.html>
35. LinkedIn <http://www.linkedin.com/>
36. LiveJournal <www.livejournal.com>
37. Microformats <http://microformats.org/>
38. Microsoft Service Agreement <http://explore.live.com/microsoft-service-agreement?ref=none>
39. Microsoft Technet <http://technet.microsoft.com/en-us/library/cc784935(WS.10).aspx>
40. Microsoft Windows Cardspace <http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx>
41. Microsoft <http://www.microsoft.com/>
42. National Policing Improvement Agency <http://www.npia.police.uk/en/10508.htm>
43. National Skills Registry <https://nationalskillsregistry.com>
44. Novell <http://www.novell.com/home/>
45. OpenID <http://openid.net/>
46. Oracle Identity Management <http://www.oracle.com/technology/products/id_mgmt/index.html>
47. Oracle < http://www.oracle.com/>
48. Orkut <http://www.orkut.com>
49. Our Human Rights Stories <http://www.ourhumanrightsstories.org.uk/>
50. Ping Identity <http://www.pingidentity.com/>
51. PrimeLife <http://www.primelife.eu/>
52. Privacy and Identity Management for Europe (PRIME) <https://www.prime-project.eu/>
53. Privoxy <http://www.privoxy.org/>
54. Ratemyteachers <http://uk.ratemyteachers.com/>
55. Red Hat Inc, Kerberos <http://www.centos.org/docs/5/html/Deployment_Guide-en-US/ch-kerberos.html>
56. Reputation Defender <http://www.reputationdefender.com/company>
57. Rotten Neighbour <http://www.rottenneighbor.com/>
58. Shibboleth <http://shibboleth.Internet2.edu/>
59. Smart Villages <http://www.smartvillages.org/hansdehar/people.htm>
60. SXIP <http://www.sxip.com/>
61. SXIPPER <http://www.sxipper.com/>
62. The Cloak <http://www.the-cloak.com/anonymous-surfing-home.html>

63. The Id Trail <http://www.idtrail.org>
64. The Liberty Alliance <http://www.projectliberty.org/>
65. The Open Group, Single Sign On <http://www.opengroup.org/security/sso/>
66. The Ramayana <http://valmikiramayan.net/>
67. Tor <http://www.torproject.org/>
68. Twitter <http://twitter.com/>
69. Typepad <www.typepad.com>
70. UIDAI <http://uidai.gov.in/>
71. University of Cambridge, The Raven/Shibboleth Service: Terms and Conditions <http://www.cam.ac.uk/cs/raven/shib-terms.html>
72. Verisign <http://www.verisign.co.uk>
73. World of Warcraft <http://www.worldofwarcraft.com/info/basics/reputation.html>
74. Yahoo! Terms of Service <http://info.yahoo.com/legal/uk/yahoo/utos-173.html>
75. Yahoo! <www.yahoo.com>