LIBERAL STUDIES JOURNAL

LIBERAL STUDIES

A Bi-Annual Journal of School of Liberal Studies, PDPU, Gujarat

Vol. 2, Issue 1
January–June 2017

ISSN 2455-9857

EXPERTS SPEAK

ARTICLES

BOOK REVIEWS

Vol. 2, Issue 1
January–June 2017

SLS
SCHOOL OF LIBERAL STUDIES

Jayadev Parida*

A Stronger Data Protection Regime for a Better Digital India

Introduction

India's presence in the cyberspace has been propelled in to digital power narratives in the global cyber diplomacy discourse.[2] To name a few, India's selection to chair the first group of governmental experts constituted to deliberate the issue of Lethal Autonomous Weapons Systems and their impact on international security[3], and as the first non-OECD country to host the Global Conference on Cyber Space. Until recently, Digital India initiative, followed by governments 'shove[4]' to promote a digital market on the base of cashless transactions has been necessitating a lot of policy reboot at a purely domestic level. In India, Cyber security is the biggest threat to national security – and something needs to be done to protect our financial, strategic and civilian networks. Similarly, some form of policy needs to be implemented wisely and precisely to manoeuvre the currency of digital age viz. DATA! Statistically, India ranks second in the world in terms of the highest number of internet users which are almost 34 per cent of a total of 1.3 billion population.

Interestingly, however, India has no clear policy frameworks to address this serious issue of data protection and individual privacy and this could prove the biggest setback in years to come. This could be precisely the reason that, Apple the most sophisticated of current technology companies has only a 2 per cent market share in India. All the Internet giants and their data servers are based under US jurisdiction; and even with a proper legal process to get information from the US via Mutual Legal Assistance Treaty, a minimum of two years will be required by the Indian government to get any information. Indian authorities have been well aware of internal and strategic impact of threats that are emanating from the cyberspace. There are, however, no national

* **The author** is Konrad Adenauer Stiftung Fellow, Otto Suhr Institute of Political Science, Freie University Berlin, Germany.

laws pertaining to data protection. The government of India should adopt a prudent and effective data protection regulation if a successful Digial India is aspired for. There is even a need for second generation laws to address this issue of cyber security and data protection. Metaphorically, privacy though a myth is not a myth at all. Privacy is an integral part of human life and should be treated as such.

The Metamorphosis[5], a world without Internet, is next to impossible. The Internet has become an essential and integral part of human life. This emerging complex 'interconnectedness' has reduced the time-space compression more than ever before. Technology is transcending geographical frontiers and threats are becoming asymmetric and unpredictable. In a span of three decades, cyberspace has highlighted a different lifestyle that has added various modern auxiliaries to our life. Internet of Things, artificial intelligence, disruptive technologies are all becoming a reality and also amplifying a Cybered life.[6] The Genesis of this life is thus dynamically synchronised into '*1s and 0s*'.[7]

This binary amalgamation is known as 'data'. Data is a set of 'information that is stored by a computer'. The Indian Information Communication Act 2000 defines data as a 'representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised 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[8].

Data can exist in different formats – as numbers or text in pieces of paper, bits and bytes stored in electronic memory. The data includes everything of a computerised human life – personal and private information of individuals, confidential and strategic documents of an organisation and critical information of a government. However, 'data protection' provides legal restrictions and guidelines on the use and misuse of data that is stored or collected by the service provider or data administrator.

"Data! Data! Data!" once cried Sherlock Holmes impatiently. "I can't make bricks without clay."[9] In the information age, data is the clay for all bricks. One cannot provide a solid output without data; the Government's needs data to protect 'national security', corporate business runs through data and also a preferred destination for all cyber criminals. Data protection became a crucial issue specifically after the Snowden revelations in 2013 about the US NSA worldwide surveillance. The revelations provide three takeaways: first, human rights specifically the right to privacy needs a special attention by establishing new global standards or modifying the existing rules. Second, the door should open for other stakeholders for regulating the Internet ecosystem i.e. the multi-stakeholder approach. Third, the UN (by establishing a new agency or revamping the existing structure) should play a bigger role in international cyber security matters.

Data protection is primarily a subject matter of the right to life and dignity, not just of business or of national security. It is quite ethical for all the stakeholders to sit at a table to discuss the fact. For instance, the peace treaty of Westphalia or the Geneva conventions has a lot of binding principles. This is not so in the case in violation of the human rights in cyberspace. This invisible world has huge humanitarian implications, and the right to privacy is an integral part of every individual.

There are three scenarios for constituting a data protection regime viz. *Right to Protect* the government should take responsibility to ensure the protection of the natural rights of all its citizens; *Responsibility to Protect* – a critical option to have a common ground, who will take the responsibility is substantially difficult to pin down. The Internet belongs to everybody and the future of the human civilisation is heavily dependent on it. Therefore, both public and private stakeholders should build trust and take responsibility to protect the individual liberty. Third and the worst case scenario is '*pay and secure*' (digital tax), pay to your respective service provider/government to give you a security blanket, and the more you pay, the more secure you will be.

For attaining a 'Digital India' (DI), the government needs to achieve three sets of parameters. First India should provide a *tech-savvy and disruptive digital infrastructure* to its tech-hungry youth population; fibre-optics is the tip of it.[10] Second, it should formulate a stronger data protection regime for its next billion netizens (NBN), digital economy and internet ecosystem at large. Third, in doing so it is the responsibility of the government to protect the socio-economic and security environment of India. In this modern day of the internet, data protection has emerged as one of the most crucial tasks that need to be addressed through a holistic approach.

This essay examines India's need for a stronger data protection regime at the advent of DI and what needs to be done to protect the NBN. Second the role of security and investment to make DI into a developed India.

Right to Privacy and Data Protection

The internet or the web-based life moves more rapidly than any other aspect of a modern civilised society. A bird's eye on the evolution of World Wide Web – Web 1.0, Web 2.0, Web 3.0, Web 4.0,[11] Web 5.0[12]…'*Web N*[13]', understandably, the Internet is among the few things humans have built that they don't truly understand.[14] Soon everyone on Earth (mainly global south) will be connected. The boom of digital infrastructure and addition of an additional 4 billion of people in to this virtual world will bring both abundant challenges and ubiquitous opportunities to other avenues of the physical world. The common future of this 'next billion' is significantly based upon uncommon terrains,[15] whereupon data protection and individual privacy are a major concern, a mere tip of a much bigger iceberg.

The advent of the digital age fundamentally reduced individual ability to protect their privacy. "Big Brother is Watching You". Beyond Orwell's Worst Nightmare,[16] they know what we prefer to eat, places to visit, likes and dislike, financial[17] and marital

status.[18] The main threat is no longer the extent of the personal information which is collected or stored by various surveillance systems of the government or private entities, but how the information is used and misused. Once collected, information can very often be accessed and misused by anyone in the world[19]. Technically privacy comes under *natural rights* of all living beings. In 1890, Samuel Warren and Louis Brandeis, first coined the term 'right to be left alone'[20] in a seminal article published by the *Harvard Law Review*. It is often understood as the first declaration of US right to privacy. This was written in response to the technology of times – the newspapers – violating the privacy of influential people by printing stories about them[21]. Shortly after Hitler Nazi regime came to power in Germany in 1933, the privacy of the citizen had undergone critical changes.[22] After the World War II the issues of 'privacy', internationally regained recognition as a fundamental part of every human being. Article 12 of the Universal Declaration of Human Rights 1948 and especially Article 8 of the European Convention on Human Rights and Fundamental Freedoms 1950 significantly underlined a global discourse on privacy issues. The tech-savvy world is demanding a new definition of privacy, which can be ensured through a global dialogue on data protection and individual privacy.

The Fifth Estate or the Wikileaks[23] had failed to convey just how important personal information is; rather it had trolled as an edge to the new journalism and exposed the US administration's gray areas over the technology and global politics. But in 2013 the Snowden expose had broken all the silence and urged to establish a stronger global mechanism for data protection and privacy. Since then the cyber ecosystem has been facing consistent makeovers. The ex-CIA systems analyst Edward Snowden revealed that Britain's electronic eavesdropping agency GCHQ and US NSA have successfully cracked much of the online encryption relied upon by hundreds of millions of people (home and foreign) to protect the privacy of their personal data, online transactions, and emails. The incident indicated that there is a lack of a legal mechanism in cyberspace. Thereafter, the stakeholders have devoted interlocutors to frame a regulation to this ungoverned domain so that security and sustainability have maintained its par.

The very fertile terrain of the Internet is fragmented by national laws. The global legal architecture is too fragile which actually helped the US NSA to execute the world wide surveillance, substantially. The US privacy laws have developed slowly, in response to society's needs, but the country still has no overarching regulations. The fourth Amendment originally enforced the notion that 'each man's home is his castle', secure from unreasonable searches and seizures of property by the government.[24] The new digital age needs to sharpen these rules further. At US common law, there were four privacy torts, which continue to exist today [25] and distinct laws that protect information related to health, video rentals, educational records, credit reports, etc[26]. The US neither has a dedicated data protection law nor a single regulatory authority for overseeing data protection law. Rather it simply has a patchwork quilt in the form of the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act of 1996, Federal Trade Commission Act, Wiretap Act, etc.[27]

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 is a first international treaty that safeguarded the subject matter of data. The Convention enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected. It also imposes some restrictions on trans-border flows of personal data to States where legal regulations do not provide equivalent protection. And also provides a ground for the national security and defence.[28] In 2001 the Council of Convention on Cyber Crime also underlined that personal data should be protected both in police sector, the area of telecommunication services, telephone services, and computer related crimes.[29]

The EU's incremental moves towards data protection is till date one of the most developed models. The EU Data Protection Directive (Directive 95/46/EC)[30] governs both automatic and manual processing of personal data for natural persons. The Directives binds the EU Member States and gives them direction to specify 'the conditions under which the processing of personal data is lawful.' The Directive serves two objectives; first it protects the fundamental rights and freedoms of natural persons and in particular, a right to privacy, with respect to the processing of personal data and secondly, it ensures that no Member States (MS) can restrict or prohibit the free flow of personal data between the MS. In order to fulfill both objectives, the Directive lays out a number of legitimate provisions.[31] On 25 January 2012, the European Commission unveiled a draft legislative to establish a unified European data protection law, i.e. General Data Protection Regulation.[32] The Regulation intends to unify data protection within the EU with a single law applicable to all MS and the Council aims for adoption in 2018.[33] This will replace the patchwork of different data protection laws currently in force in all 28 MS.

The Organisation for Economic Co-operation and Development (OECD) in 1980 adopted sets of Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. This provides a soft ground of understanding between the member states while overseeing the differences between the national laws and policies. It also underlined that automatic processing and trans-border flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices, this can contribute to economic and social development.[34] As the size of data (big data) is changing, old policies need to be reshaped accordingly. In 2014, Microsoft asked the Oxford Internet Institute to organise a small working group of senior leaders with experience in data protection regulation to review the 1980 OECD Guidelines and updated them according to the 21st century.[35]

The Asia-Pacific Economic Community (APEC), published the Privacy Framework published in 2004.[36] APEC is a forum for facilitating trade and investment in the Asia-Pacific region composed with 21 diverse member countries. In 2007 Peter Fleischer, Google Privacy Counsel, also endorsed the Framework. But the principles are ambiguous with respect to their effect and are capable of a vast number of interpretations and implementations and not at all mandatory; China, for instance, has already indicated

that it has nothing do with them. On the other hand, lack of detail in the Framework makes it a shaky foundation that risks creating national privacy laws and rules that would be inconsistent with each other and far weaker than Europe's traditional approach to the subject.[37]

'I Agree' is a costly affair.[38] The 'Safe Harbour' is a special regulation adopted by the EU to maintain a strict privacy protection for its citizens. It allows the third party to do business within EU if they meet 'adequacy' standard for privacy and data protection. Since 2000, the US Department of Commerce has collaborated with the European Commission to provide an adequate level of protection for the EU business that transfers personal data to the US companies so as to enable them to comply with the data export requirements of the EU Directive. The Snowden disclosure has emerged as a flashpoint; similarly, the US data protection and privacy standards are lower than their European counterparts. Maximillian Schrems affairs and Press Release No 117/15[39] of the Court of Justice of the European Union significantly posed a serious concern between the natural allies. The future of the US-EU Safe Harbour is unsafe now.

The recently emerged crisis over the Safe Harbour, has raised a very pertinent question about what should the future of privacy and data protection be. It is possible to frame a legal mechanism to protect the data and that is only possible through 'trust'. Some testimonies can be drawn from now that all the stakeholders should work for an international cooperation rather than harmonising their own national laws. The old cliché of diplomacy and 'sovereignty' needs to be redefined because internet belongs to all and free, open and secure Internet is the driving motto of this century. On the other hand, Soft Laws (standardisation) and Mutual Legal Assistance Treaty could be considered as a significant domain to work for data protection and privacy. Similarly, there is a need for global architecture, so the UN should create a new set up specifically to deal with the issue of data protection.

Data Protection and Privacy in India

'Privacy' has been a contested subject in the Indian legal and political architecture, the reason is the Fundamental Rights chapter of the Constitution that reveals no mention of the word 'privacy', or anything that seems like a 'right to privacy'. The Indian judiciary and the Supreme Court in particular, have dealt with the issue of privacy, both as a fundamental right under the Constitution and as a common law right. The common thread through all these judgements of the Indian judiciary has been to recognise a right to privacy, either as a fundamental right or a common law right, but to refrain from it in iron-clad terms.[40] The very first case to lay down the contours of the right to privacy in India, was the case of *Kharak Singh v. State of Uttar Pradesh (1964) SCR (1) 332*. A fascinating development in the Indian Constitutional jurisprudence is the extended dimension given to Article 21 by the Supreme Court in post-Maneka era. The Supreme Court has asserted that Article 21 is the heart of the Fundamental Rights.[41] However, the Article 21 is safeguarding the right to privacy of Indian citizens.

The ubiquity of data transfers over the Internet is exposing individuals to more privacy risks. On the other hand collecting the data directly entered by the users or through their actions without their knowledge to generate financial gain out of data is also another major threat to data privacy. Data protection is a critical aspect of knowledge based society. The opportunities of the Indian market is exponentially attracting business and investment that also gaining currency between global stakeholders. Unlike EU, India does not have a strong data protection law that sometimes creates a hurdle to establishing a new business. However, just as in the case of the US, India has various laws that govern the data protection.

The Telecom Authority of India protects consumers by requiring that telecommunications service providers guard subscriber privacy whenever national security is not implicated.[42] The Public Financial Institutions Act on 1993 protects confidentiality in bank transactions.[43] The Information Technology Act (IT Act) of 2000 addresses computer crimes, including hacking, damaging computer source code, breaching confidentiality and viewing pornography.[44] Moreover, cyber security and data protection measures are supported by various enactments viz. the Indian Telegraph Act, 1885, the Indian Contract Act, 1872, the Specific Relief Act, 1963, the Public Financial Institutions Act, 1983, the Consumer Protection Act, 1986 and the Credit Information Companies (Regulations) Act, 2005.

The IT (Amended) Act 2008 has 'strengthened'[45] the data protection regime in India[46]. Section 43A deals with implementation of reasonable security practices for *sensitive personal data or information* and provides for the compensation of the person affected by *wrongful loss or wrongful gain*. Section 72A provides for the imprisonment for a period up to 3 years and/or a fine up to Rs. 500,000 for a person who causes *wrongful loss or wrongful gain* by disclosing personal information of another person while providing services under the terms of lawful contract.[47]

In June 2011, the Ministry of Communications and Information Technology's notification underlines a new privacy package that included various new rules that apply to companies and consumers: The Information Technology Rules (Reasonable Personal Data or Information) 2011. A key component of these rules was that any organisation processing personal information in India requires written consent before undertaking certain activities and must implement reasonable security policies and process[48]. The new rules added a caveat into the data protection regime viz. Eight Sensitive Personal Data or Information[49] that needs to be protected. The technology rules have underlined a clear distinction between the 'Right to Information' and 'Right to Privacy' (data protection).[50] The intention of the Indian Government is to enhance the data security and privacy in the country and it feels that this is a crucial step to promote offshoring in India. However, the actual nature of these rules does not completely solve the original purpose.[51]

In 2013 the Centre for the Internet & Society proposed a bill 'The Privacy (Protection) Bill 2013'. The bill 2013 does not provide any definition of 'privacy',

however, it focused on the protection of personal and sensitive personal data of persons.[52] On the other hand, the revised CIS Privacy Bill gives a free pass to NASSCOM and Big Data.[53]

During 2011-2013 there were three significant proposals for a comprehensive data privacy law in India but none gained the endorsement of the previous government.[54] There is a need for a comprehensive and strong data protection regime which got a new momentum in February 2014, viz. "The Right to Privacy Bill 2014". The proposed bill extends the right to Privacy to all residents of India including those residing in *Jammu and Kashmir*, the bill furthermore recognises the Right to Privacy as a part of Article 21 of the Indian Constitution.[55] For the present government, cyber security is a critical issue and thus the government needs to adopt a strong law which will ensure privacy and data protection. Moreover, the future of digital revolution in India is heavily reliant on how the government and private sectors are implementing their data protection and privacy regulations.

Securing Digital Market in India

Indian market has shown a strong commitment to transform via digital revolutions and at the same time there is a need to construct a global system that can accommodate and allow for such a transformation. Access, Voice and Opportunity must not be more cumbersome for the 'next billion.' And, this also means more responsibility for the Indian government.[56] According to a survey conducted by *Observer Research Foundation, 'Digital India: Aspirations high in smaller cities than in metros*. People in smaller cities of India were more hopeful about the prospects of digital technologies than the people in big cities and metros which are traditionally thought of as 'tech savvy'. The survey, done as part of the CyFy 2015 State of the Debate to discern key trends in the usage of the information services in the digital economy among Indians, also found that for Indians who spend nearly two hours on an average on the internet every day, Facebook accounts for a lot of the time spent online. The survey was conducted in ten 'million-plus' cities with an average population of 6.1 million. These surveys were conducted at supermarkets in each of the cities to target the middle class. On an average 50 respondents from each city participated in the survey. The survey found that while Indians distrust cyberspace for storage of their personal data, it does not hinder their participation in online markets.[57] A testimony of this survey suggests that the future of the revolution is relying on – *e-commerce, digital economy and app-society*.[58] Another research suggested that by 2020, India's entertainment and media industry will be able to clock over USD 40,000 mn.[59]

Clearly, the Internet is mainstreaming in India's growth, the advent of low-cost ICT gadgets like smartphones has been nourishing the app-society and economy. India's internet user base was 462 million in 2016[60], similarly the e-Commerce industry is swiftly rising, changes can be seen over the years. E-commerce sector in India has grown by 34 per cent, compound annual growth rate since 2009 has touched $16.4 billion in 2014.[61] As of now India is the second largest Internet user in world, and

though the penetration of e-commerce is low compared to western markets, it is growing exponentially and adding around 6 million new entrants every month[62].

Innovative service offerings by the e-commerce industry like one-day delivery, big billion day, 30 day replacement warranty, Cash on Delivery (CoD), cash back, mobile wallets, etc has been significantly promoting new domains of business all over India. On the other hand, through this India Post has also been regaining its significance; in 2014, the Indian Post collected INR 2.8 billion trough CoD option of payment.[63] Similarly, low average broadband speed and flat average internet speed, the absence of e-commerce laws, low entry barriers, rapidly changing business models, urban phenomena, shortage of manpower and customer loyalty[64] are some challenges to the *horizontal and vertical growth* of e-commerce in India.

One of the biggest challenges in this e-transformation is data security. To address this, Indian industry has taken proactive steps, but the threat landscape is dynamic and requires organisations to keep upgrading their security programmes as per demands. New technologies bring new security threats, new models, vulnerabilities and risks along with new opportunities. In a cybered world security is not a single window activity but an ongoing process. To ensure this, data protection and security will remain to be key enablers.

In the next 3 years digital expansion will be adding the *next great billion* to India's digital ecosystem. This will significantly reduce the numeric value of digital haves and have nots. To achieve this milestone, the government has envisaged nine digital pillars,[65] but all this will require a huge magnitude of investment and the Indian market has a huge potential in this regard. The visit of the Indian Prime Minister to the Silicon Valley is another promising, open door policy for greater digital investment. The promise of the Valley gives two headways: a larger investment in digital market and a rise of the 'Natural Language Processing' industry, which is minimal in the Indian context.

Digital India needs strong and dynamic cyber security architecture. But India has failed to deliver a structural approach to cyber security. Despite being the third biggest target[66] among cyber criminals at a global level, India does not have a cyber strategy or unified cyber command to look after its netizen privacy and national security.

The Way Forward

The recent demonetisation saga, rise of new e-payments platforms and the government push for Aadhaar linked transactions has a lot to do with data protection regulations. India will be the first country to *glocalise*[67] the digital ecosystem. On the other hand, an advanced model of cyber security architecture is the need of the hour. That can be possible through a second generation data encryption policy, data protection and privacy laws. A wise and tech-savvy decision will be more helpful to develop a truly successful Digital India.

As per the various estimations, 70 per cent of Indians are living in rural India; Digital transformation will bring a new platform to them. Most of the time cyber incidents

become paramount due to human errors.[68] Behind the computer screen, ethics play a very insignificant role. It is also the duty of the government as well as the business stakeholders to invest and create 'ethics' in cyberspace. A developed India is possible only if the digital India(ns) successfully manoeuvre digital investment along with human ethics and security.

On the other hand, after 2019, the present size of data will increase exponentially. In view of this, the present government should first create a data protection regime to ensure privacy and security for all. Secondly, a dedicated and autonomous governmental body should be formed to deal with the privacy and data protection. Nonetheless, a stronger data protection regime will bring a positive and progressive growth to Digital India.

Notes

1. Samir Saran, "A Reluctant Digital Power Emerges From the Shadows", *The Wire*, 22 December 2016.
2. Arun Mohan Sukumar, "India to Chair UN Group on 'Killer Robots', Open New Page on Arms Control Diplomacy", *The Wire*, 19 December 2016.
3. Mihir Sharma, "India Needs a Nudge, Not a Shove", *Bloomberg*, 16 February 2017.
4. Franz Kafka, *The Metamorphosis*, (Kurt Wolff, Leipzig, 1915), a 20th century fiction that had deconstructed the social system in differently. It has been used here as a metaphor to see study the digital life how it shaping the ideas, technology, policy, strategy and conflicts.
5. Chris Demchak, "Conflicting Policy Presumptions about Cybersecurity: Cyber–Prophets, –Priests, –Detectives, and –Designers, and Strategies for a Cybered World," Atlantic Council, *Issue Brief*, 12 August 2010, http://www.atlanticcouncil.org/images/files/publication_pdfs/403/Demchak-brief.pdf.
6. Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*, USA, Paeger, 2013.
7. Information Communication Act, No 21 of 2000.
8. Sir Arthur Conan Doyle, *The Adventure of the Copper Beeches*, Happer & Brothers, 1892, pp. 289.
9. Small Satellite can be used as new tool for Digital India, see, Vignan Velivela, "Small Satellite Constellations: The Promise of 'Internet for All'", *ORF Issue Brief*, No. 107, September 2015.
10. Sareh Aghaei1, et al., "Evolution of the World Wide Web: From Web 1.0 to Web 4.0", *International Journal of Web & Semantic Technology*, vol. 3, no. 1, 2012, pp. 1-10.
11. Flat World Business, "Web 1.0 vs. Web 2.0 vs. Web 3.0 vs. Web 4.0 vs. Web 5.0 – A bird's eye on the evolution and definition", accessed 27 October 2015, https://flatworldbusiness.wordpress.com/flat-education/previously/web-1-0-vs-web-2-0-vs-web-3-0-a-bird-eye-on-the-definition/.
12. It is unknown to everybody what would be the future of Web.
13. Eric Schmidt and Jared Cohen, *The New Digital Age*, London, John Murray, 2013.
14. "Theme of CyFy 2015", the India Conference on Cyber Security and Internet Governance, 14-16 October 2015.
15. Marjorie Cohn, "Beyond Orwell's Worst Nightmare", *The Huffington Post*, updated 02 April 2014, accessed 27 October 2015, http://www.huffingtonpost.com/marjorie-cohn/beyond-orwells-worst-nigh_b_4698242.html?ir=India&adsSiteOverride=in.

16. Tom de Castella and Kayte Rath, "Prism and privacy: What could they know about me?", *BBC News Magazine*, 12 June 2013, accessed on 27 October 2015, http://www.bbc.com/news/magazine-22853432.
17. BBC India, "The Indian matchmakers targeting divorcees", 11 May 2015, accessed on 27 October 2015, http://www.bbc.com/news/world-asia-india-32547360.
18. Amitai Etzioni, *Privacy in a Cyber Age: Policy and Practice*, USA, Palgrave Macmillan, 2015.
19. Samuel Warren and Louis Brandeis, "The Right to Privacy", *Harvard Law Review*, vol. IV, no. 5, 1890, accessed on 27 October 2015, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.
20. Data Security Council of India, "Legal Framework for Data Protection and Security and Privacy Norms", *Consultation Paper Submitted to DoPT, 5 July 2010*, accessed on 27 October 2015, https://www.dsci.in/sites/default/files/Legal%20Framework% 20for%20Data%20Protection%20and%20Security%20and%20Privacy%20norms_0. pdf.
21. "The emergence of privacy as a human right", accessed on 27 October 2015, https://www.dataprotection.ie/documents/teens/cspe%20resource%20booklet/Section_2_-_Privacy_as_a_Human_Right.pdf
22. A movie based on WikiLeaks and Julian Assange.
23. US Constitution Fourth Amendment, accessed on 29 October 2015, https://www.law.cornell.edu/constitution/fourth_amendment.
24. Ariel E. Wade, "A New Age of Privacy Protection: A Proposal for an International Personal Data Privacy Treaty", *George Washington International Law Review*, no. 42, 2010, pp. 659-685.
25. *Ibid.* p. 662.
26. Rosemary P Jay, *Data Protection and Privacy 2014*, London, Hunton & Williams, accessed 15 September 2015, https://www.hunton.com/files/Publication/1f767bed-fe08-42bf-94e0-0bd03bf8b74b/Presentation/PublicationAttachment/b167028d-1065-4899-87a9-125700da0133/United_States_GTDT_Data_Protection_and_ Privacy_ 2014.pdf.
27. Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981", accessed on 28 October 2015, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.
28. Council of Europe, "Convention on Cyber Crime, 2001", accessed on 28 October 2015, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
29. European Council, "Directive 95/56/EC of the European Parliament and of the Council", 24 October 2015, accessed on, 20 September 2015, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
30. *Ibid.*
31. European Commission, "Regulation of the European Parliament and of the Council", 25 January 2012, accessed on 25 September 2015, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
32. Ben Rossi, "New EU Data Law's Go-live date Finally Revealed - and why it costs will run into billion", *Information Age*, 12 August 2015, accessed on 29 October 2015, http://www.information-age.com/technology/information-management/123459991/new-eu-data-laws-go-live-date-finally-revealed-and-why-its-costs-will-run-billion.
33. Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, accessed on 25 October 2015, http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm#part1.

34. Fred H. Cate, "Data Protection Principles for the 21st Century Revising the 1980 OECD Guidelines", March 2014, accessed on 29 October 2014, http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf.
35. Asia-Pacific Economic Community, "APEC Privacy Framework, 2004", accessed 25 September 2015, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx .
36. Chris Pounder, "Why the APEC Privacy Framework is unlikely to protect privacy", 15 October 2007, accessed on 29 October 2015, http://www.out-law.com/page-8550.
37. Alexis C. Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days", 1 March 2012, http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/, accessed on 29 October 2015.
38. Court of Justice of the European Union, "Maximillian Schrems v Data Protection Commissioner", Press Release No 117/15, Luxembourg, 6 October 2015, accessed on 29 October 2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.
39. Government of India, "Report of the Group of Experts on Privacy", *Planning Commission*, 16 October 2012.
40. "Right to Privacy Under Article 21 and the Related Conflicts", 22 January 2014, accessed on 30 October 2015.
41. The Telecom Regulatory Authority of India Act, No. 24 of 1997.
42. The Recovery of Debts Due to Banks and Financial Institutions Act, No 51 of 1993.
43. IT Act 2000.
44. The Centre for Internet & Society, "IT Act and Commerce", 11 August 2009, accessed on 30 October 2015, http://cis-india.org/internet-governance/blog/it-act-and-commerce.
45. Kamlesh Bajaj, "Data Protection Regime Beefed Up", 20 January 2009, accessed on 30 October 2015, https://www.dsci.in/sites/default/files/data_protection_regime_ beefed_up_livemint_20th_jan_2009.pdf.
46. *Ibid.*
47. CRID, "First Analysis of the Data Protection Law in India", University of Namur, accessed on 30 October 2015, http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf.
48. Password, financial information, health information, sexual orientation, medical records and history, Biometric Information, etc.
49. Ministry of Communications and Information Technology, "Information Technology (Reasonable security practices and procedures and sensitive data or information) Rules, 2011", 11 April 2011, accessed on 30 October 2015, http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.
50. Patrick S. Ryan, et al., "Regulation of the Cloud in India", *Journal of Internet Law*, vol. 15, no. 4, 2011, pp. 7-17.
51. Neeraj Dubey, "The Privacy (Protection) Bill, 2013", *PSA Legal Counsellors*, 8 November 2013, accessed on 30 October 2015, http://www.mondaq.com/india/x/273736/Data+Protection+Privacy/Secret+Agreement+Fragile+Evidence.
52. Prashant Reddy, "Revised CIS Privacy Bill gives a free pass to NASSCOM and Big Data", 16 October 2013, accessed on 30 October 2015, http://spicyip.com/2013/10/revised-cis-privacy-bill-gives-a-free-pass-to-nasscom-and-big-data-2.html.
53. Graham Greenleaf, "India's Data Protection impasse: Conflict at all levels", *Privacy Laws & Business International Report*, no. 127, 2014, pp. 23-24.

54. Centre for Internet and Society, "Leaked Privacy Bill: 2014 vs. 2011", 31 March 2014, accessed on 30 October 2015, http://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011.
55. Samir Saran and Mahima Kaul, "The 'I' in the Internet Must Also Stand for India", *The Wire*, 24 June 2015.
56. Observer Research Foundation, "Digital India: Aspirations high in smaller cities than in metros", *CyFy 2015 State of the Debate*, 20 October 2015, accessed on 29 October 2015, http://www.orfonline.org/cms/sites/orfonline/modules/report/ReportDetail.html?cmaid=89741&mmacmaid=89742.
57. App-Society is a metaphorical society – exponentially use of smart phone and application based service will make this metaphor into reality in DI.
58. PWC, India's entertainment and media industry to clock over US$40,000mn by 2020: PwC Report.
59. *The Economic Times*, 3 September 2015.
60. PwC, "eCommerce in India Accelerating growth", February 2015, accessed on 30 October 2015, http://www.pwc.in/assets/pdfs/publications/2015/ecommerce-in-india-accelerating-growth.pdf.
61. *The Times of India*, 20 November 2014.
62. *The Times of India*, 30 November 2014.
63. EY, Re-birth of e-Commerce in India, accessed on 30 October 2015, http://www.ey.com/IN/en/Industries/Technology/Re-birth-of-e-Commerce-in-India.
64. Government of India, "Digital India", accessed on 30 October 2015, http://www.digitalindia.gov.in/content/programme-pillars.
65. *The Business Standard*, 25 April 2014.
66. "glocalization", http://searchcio.techtarget.com/definition/glocalization, accessed on 31 October 2015
67. Fran Howarth, "The Role of Human Error in Successful Security Attacks", 2 September 2014, accessed on 31 October 2015, https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/.