Chapter 6
Privacy, Control and the Law

6.1 The Ungovernable Internet

e-Governance is primarily is about accessing services provided by governments online. One may do it from a home Internet service or from cyber cafes or any other computer which is away from home. To access a service, there are certain authentication requirements such as name, address, email, telephone number, password and sometimes bank details if financial transactions such as property registration, tax payment, investments or account management are to be done. Sometimes people go to public computers or ATM machines and do not log off, or many such computers are fitted with cookies to record the user's communication, password and address book. In e-governance, password is the key to one's privacy; once this is procured by an unauthorised intruder into one's e-machine, then the access may be endless, unlimited, leading to some of the worst forms of financial and physical harassment and harm. The hacked data may also be used to send unwarranted, obscene or hate mails with the purpose of inciting communal or racist violence, disturbances or misinformation. Currently, this is one of the major concerns of law administering agencies since both citizens and the law are not in a position to capture the complete dimension, process and impact of such a crime. More so because the digitised content cannot be deciphered by existing terrestrial laws. Many questions emerge on the theme which would be discussed in this chapter such as why should the Internet be governed, who should govern the Internet, and, lastly, how can accountability of users be balanced with their autonomy? The fundamental issue which has been creating fuzziness on the issue of authority, control and privacy is the fact that both the 'Internet' as well as 'governance' are multifaceted and remain till today multi-definitional about which the holistic understanding is one big casualty.

The policymakers in the developing countries are now beginning to see the inherent dangers of Internet misuse when large-scale disruptions in cities and in personal and business lives can be caused by mischievous and hate content passed on emails or on social media sites. Governments have been readying to confront the issue and to enact rules to hold intermediaries responsible for user-generated

A. Singh, *A Critical Impulse to e-Governance in the Asia Pacific*,
DOI 10.1007/978-81-322-1632-2_6, © Springer India 2013

content that is allegedly obscene, infringing, defamatory or otherwise illegal. This has brought down business of cyber cafes which are closing down. Cyber cafes have been responsible for the success of e-governance programmes in Gujarat, Hyderabad, Bangalore and other emerging cyber cities across the world. Of those many new areas of employment which came to the Internet-skilled youth in the last decade and a half, cyber café had been one of the frontrunners. A large number of them have already closed down. More than the regulations which they are to follow are the constant surveillance visits of police to their cafes which disturbed user clients and this also increased rent seeking from these places. If local law enforcement authorities and international rights holders associations have their way, intermediaries will be saddled with strict obligations to take down (or, worse, monitor) content and retain user data for investigatory purposes, turning litigation-averse intermediaries into de facto censors (Rizk 2011).

Internet governance is becoming a concern for nations and international agencies such as the International Telecom Union (ITU), ICANN and the WSIS which have been occupied since 2003 to find a reasonable solution to the whole complicated problem. The problem is acute when the law itself comes in question since terrestrial and cyber laws would be different at many points even though they converge sometimes at their contours. There are issues of boundary, sovereignty and control. Thus to find laws which are workable across the concept of boundaries, they could be self-regulated rather than under a single institutional control such as what exists today under the USA. Whatsoever be the structure of such a cyber law, it indicates a paradigm shift in the understanding of law. The gist of the paper 'Law and Borders: The Rise of Law in Cyberspace' by David R. Johnson and David G. Post is that the Internet should be self-governed rather than being governed by one particular state. This would then define citizenship of Internet users not by boundaries but by location in cyber space. The authors forecast that 'Separated from doctrine tied to territorial jurisdictions, new rules will emerge, in a variety of on-line spaces, to govern a wide range of new phenomena that have no clear parallel in the nonvirtual world. These new rules will play the role of law by defining legal personhood and property, resolving disputes, and crystallizing a collective conversation about core values' (1996, p. 1367).

A recent book on the subject *The New Digital Age (2013)* suggests many insights on the subject of regulations, and the authors being the Executive Chairman Eric Schmidt and Google Ideas Director Jared Cohen have added a form of passion in suggesting ideas which demand understanding of the Internet by policymakers. They start by highlighting a major challenge about the governability of Internet as they initiate the discussion with rapt comments on the state of things to come over the digital platform, 'Internet is among the few things humans have built that they don't really understand. What began as a means of electronic information transmission-room sized computer has transformed into an omnipresent endlessly multifaceted outlet of human energy and expression' (2013, p. 3). Internet by its very nature is difficult to control as once initiated the packets of data keeps moving which is called 'packet switching' which moves forward from nodes to various nodes which are accessed by multiple users and in multiple ways. The data is not

transferred as it is but it is coded in binary numbers which need to be deciphered before they are regulated. Therefore it is 'the largest experiment involving anarchy in history' (Schmidt and Cohen 2013, p. 3). As law enforcing agencies navigate the rich virtual landscape of Internet, they pass through the online scams, e-groups of militants and religious fundamentalists with their targeted, maligning and malicious campaigns. One would agree to a point with the Google authors that Internet is the largest 'ungoverned space' (p. 3) because it is a less understood phenomenon with a high traffic of innocents in the midst of scheming pirates. Internet governance is the demand of the day, but it should also be kept out of the passion for governance by many governments. Due to the combination of two equally 'misunderstood' terms such as the Internet and governance, the arena is vulnerable to misuse by every regulator, be it the United Nations, Internet multinationals and country governments. John Mathiason sums up the problem of the prevalent ignorance about an understanding of both the Internet and governance as 'when internet is defined the aspects that can be regulated can also be defined. When governance is defined the limits of regulation will also be set out' (2009, p. 6).

6.2 Growing Government Censorship of the Internet

After the great Watergate Scandal in the USA which led to the resignation of President Nixon, it was realised that individual privacy had become more vulnerable with the coming of the electronic communication. In passing of the Privacy Act[1] of 1974, the Congress[2] found that 'the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies' and that 'the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information'. From the 1970s to the present, electronic communication has moved much further from simply recording on cassettes to public display of multiparty communication like on Facebook and Twitter, and the boundary reach of such communication could be unimaginable by any law-making agency.

The debate on control has been exacerbated by many incidents of administrative overstepping in resolving electronic communication conflicts across the world. In India during November 2012 Shaheen Dhada, a young college student, was arrested by the Mumbai Police for posting a message on Facebook to her friend Rinu Srinivasan. The two girls were charged under Section 295A for hurting religious sentiments, apart from Section 66(a) of the Information Technology Act 2000. The comment posted was

[1] The Privacy Act of 1974 , 5 U.S.C. § 552a.

[2] Public Law No. 93–579 (1974).

> With all respect, everyday thousands of people die, but still the world moves on. Just due to one politician dies a natural death, everyone just goes bonkers. They should know, we are resilient by force, not by choice. When was the last time, did anyone showed some respect or even a two minute silence for Shaheed Bhagat Singh, Azad and Sukhdev or any of the people because of whom we are free living Indians? Respect is earned, given and definitely to forced. Today, Mumbai shuts down due to fear, not due to respect.

The wrongful arrest incited public protest, and even the Chairman of the Press Council of India Justice Markandey Katju criticised the police high-handedness and noticed the mischief which had gone behind misinterpreting and misusing the provisions of law by the police. The girls were later freed and the four police officers were indicted after an internal enquiry.[3]

Asian governments have been showing an increasing trend towards controlling online data which is somewhat an emerging negative tendency against Internet users and is likely to affect the advancement of e-governance. As terrestrial laws are applied to deal with Internet issues, there are more problems which affect individual freedom as boundaries are unlimited and jurisdictions undefined. Notwithstanding the realisation that even though the basic framework of law agencies is more or less similar in the treatment of 'privacy' and 'theft' or 'misuse of information', the approach would be greatly different. Internet is a free mode of communication for the dissemination of knowledge in dialectics or in continuous growth. Thus the provisions which prohibit 'hate speech' in several sections of the Indian Penal Code and the Code of Criminal Procedure to restrict the freedom of expression may prove a disaster if applied on communication over the Internet. Section 95 of the Code of Criminal Procedure gives to government the right to declare certain publications 'forfeited' if the 'publications…..appear to the State Government to contain any matter, the publication of which is punishable' under Section 124 A or Sections 153A, 153B, 292 and 293 or Section 295A of the Indian Penal Code. Section 295A says, 'Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of citizens of India [by words, either spoken or written or by signs or by visible representations or otherwise]insults or attempts to insult the religion or the religious beliefs of that class shall be punishable with imprisonment of either description for a term which may extend to [3 years] or with a fine or with both'. Indian Penal Code was enacted in 1927 but continues to be a dominant paradigm for the police to take action against crimes of 'free expression in print or otherwise'. The abuse of Section 66A of the Information Technology Act of 2000 which is not limited to procedural issue of arrest on a scale of 'grossly offensive' acts has been ignored.

The amendments to the Information Technology Act in India have brought much relief to the Internet users. The language of Section 66 'computer related offences' has been revised. The Report of the Expert Committee (2005) expressed that 'sometimes

[3] Mumbai Mirror, (2012, 19 November) 'In Palghar, cops book 21-year-old for FB post', Mumbai and The Hindu, (2012, 19 November)' Mumbai shuts down due to fear not respect', New Delhi edition.

because of lack of knowledge or for curiosity, new learners/Netizens unintentionally or without knowing that it is correct to do so end up doing certain undesirable acts on the Net. For a country like India where efforts are being made to enhance the positive use of internet and working towards reducing the digital divide, it needs to be ensured that new users do not get scared away because of publicity of computer related offences',[4] The Committee warned that the IT Act in order to ensure that it promotes the use of e-commerce, e-governance and other online uses has been cautious not to use the word cybercrime in the text. Section 43, dealing with 'Penalties and Adjudication on data security and privacy', has been revisited to ensure that a distinction is made between causal comments and gross offences while at the same time adding Section 43A for bringing greater clarity on institutional security policy on the issue of hacking of computer-based 'sensitive personal data information'(The Gazette of India 2009, p. 6). A larger part of the language of Section 66A of the amended IT Act has been borrowed from Section 127 of the UK's Communication Act 2003. This section should be read in line with the famous House of Lords verdict[5] which read, 'The test is whether a message is couched in terms liable to cause gross offence to those to whom it relates'. It further said that the words in question must be judged by applying 'the standards of an open and just multiracial society' and 'taking account of their context and all relevant circumstances'. About a yardstick to judge such offences, the verdict suggested, 'there can be no yardstick of gross offensiveness otherwise than by the application of reasonable enlightened, but not perfectionist contemporary standards to the particular message sent in its particular context'. Judging by these standards, much of the free expression of youngsters over the net will not be treated as a 'gross violation' and would indicate that 'policing of the type taking place across the Asian region is a gross violation of personal liberty and free expression'. Matters are worsened when the larger framework of an authoritative state invokes terrestrial laws to strengthen a cause for punishment, such as the 'bailable' Section 66A of the IT Act was combined with Section 295A (deliberate, malicious acts intended to outrage religious feelings or any class by insulting religion or religious beliefs) and Section 505 (statements conducing to public mischief) just to make the offence 'non-bailable'. The bench indicated a 'motive' or 'mens rea' behind the incident of Palghar against the Mumbai girls. The issue which emerges out of the law enforcement agencies' failure to understand and interpret the nature of offence and the language of law in the context of cyber communication, respectively, has become a major challenge for the Indian judiciary.

In this context, a detailed elaboration of the above-mentioned judgement from the Royal Court of London straightens the twisted problem of freedom and control over the net. It substantially settles the whole issue which has been perplexing the Asia Pacific emerging economies where the ideology and expressions of the

[4] Report of the Expert Committee (2005) Proposed Amendments to Information Technology Act 2000, New Delhi: DIT, Ministry of Communication and Information Technology, GoI.

[5] Paul Chambers and Director of Public Prosecutions [2012] EWHC 2157 Case No: CO/2350/2011 Date: 27/07/2012.

government and the aspiring younger generation have been put against each other and are threatening to clamp down upon the technology of the Internet. Even the fast modernising Malaysia, Hong Kong, Sri Lanka and China, notwithstanding its fast strides into global markets and Internet industry, have been leading in regressive state policies against the Internet. To deliver the judgement, even the hon'ble judges the Lord Chief Justice of England and Wales Mr. Justice Owen and Mr. Justice Griffith preferred to clarify the understanding on the social media site particularly 'Twitter' which was in question before the court. 'Twitter' enables its users to post messages called 'Tweets' on the 'Twitter' interne and other sites. These are jokes, gossips, opinions, assertions and descriptions which are both good and bad. As in the FB Palghar Case of Mumbai girls or the UK's Paul Chamber's Case, the issue had been one in which the prosecution had failed to interpret the online loose 'comment' in the context of online expressions used on these social media sites. The case came up as an appeal against the Magistrate Court's upholding of the conviction against the 'Twitter user' for sending by a public electronic communication network a message of a 'menacing character' contrary to Section 127(1) (a) and (3) of the Communications Act 2003 (the Act).

The appellant was to fly to Belfast from Doncaster Robin Hood Airport to meet the 'Twitter' friend identified as 'Crazycolours' on 10 January 2010. Due to bad weather conditions, the flights were cancelled. This incited anxiety and anger spurting into remarks such as 'I was thinking that if it does then I had decided to resort to terrorism' and 'I am blowing the airport sky high'. The public prosecutor had placed the message under 'grossly offensive' category, whereas the hon'ble judges laid down a criteria for such a category. The judgement read, 'In short, a message which does not create fear or apprehension in those to whom it is communicated, or who may reasonably be expected to see it, falls outside this provision, for the very simple reason that the message lacks menace'.[6] What is the mens rea[7] for an offence of sending a message of menacing character contrary to Section 127(1)(a)? In particular, (a) Is Section 127(1)(a) (read according to convention canons of construction or with the benefit of Article 10 ECHR[8] and Section 3 of the Human Rights Act 1998) a crime of specific intent? (b) Is the Prosecution required to prove as part of the mens rea of the offence that the person sending the message intended to put another person in fear? (c) If the answer to (b) is no, is it sufficient for the prosecution to prove that the person sending the message realised that his message may or might be taken as menacing, or must the prosecution prove that he realised that it would be taken as menacing by a person of reasonable firmness aware of all the relevant circumstances?

[6] Paul Chambers and Director of Public Prosecutions [2012] EWHC 2157 Case No: CO/2350/2011 Date: 27/07/2012.

[7] Mens rea (or guilty mind) is a Latin term which is used to explain the motive behind the crime, suggesting criminal liability as 'the act is not culpable unless the mind is guilty'. Besides, there must be an 'actus reus' (or guilty act) accompanied by mens rea to constitute the crime. Technically, there is no criminal liability attached to a person who acted without mental rea.

[8] ECHR is European Court of Human Rights.

The best thing which has emerged out of this case is that the Director of Public Prosecutor seem to have become enlightened with the participation in the court discussions crystallising into a judgement. He preferred to issue guidelines on social media cases for prosecutors so that they have a standard set of understanding about the distinction between free speech and criminality.[9]

However, the judicial verdict of the British Court has not influenced the Asia Pacific judicial pronouncements except that of Indian Judiciary. In the Palghar Facebook Case in India, the Court had taken a pro-freedom approach, but this has not been happening around the other Asian countries. It is being witnessed throughout Asia that efforts to control Internet intermediaries with new sets of rules have unnecessarily constrained the performance of Internet service providers (ISPs), online service providers such as Twitter and Google or cyber cafes. In fact the number of cyber cafes is reducing in the suburbs of big cities as the police and other law enforcing agencies have created a scare that they would be responsible for the harmful, obscene, malicious and secessionist content of the user at the café. The state has been strengthening itself against the new found freedom platform which the Internet has given to the world. The Internet intermediaries (ISPs and online service providers like 'Twitter, Facebook and Google') increase the Internet access cost proportionate to the regulations imposed upon them thereby affecting cost of access anywhere outside the home. Yet the intermediaries have also been subjected to the need for 'disclosure of Internet users' personal data'. In Malaysia, the government has brought amendments to the Electronic Commerce Act 2006 to compel online marketplace operators to maintain proper records of their sellers which could be relied upon for the purpose of investigations. Even the Computing Professionals Act 2011 is moving towards restricting Internet freedom.

The ICT Acts in South Asian countries are being amended towards stricter punishments. The Bangladesh ICT Act of 2006 provides legal recognition and security of information. Pakistan released provisions of the Ordinance No. XIV of 2009 for the prevention of electronic crimes such as the criminal access to computer data, its damage or system damage and also cyberterrorism. Malaysian government has also been proactively restricting Internet freedom as Malaysia emerges to become the sixth most vulnerable country to cybercrimes and misuse of the Internet for various cross-border illegal activities such as drugs, human trafficking, financial fraud and money laundering (The Star 16th May, 2013).

6.3 Grassroot Movements for Internet Freedom

Why would people share their personal data if there is little trust left in governments on its misrepresentation and misuse? Even the issue of misinterpretation of content language and the same outdated patriarchal and rent-seeking administration and law

[9] http://www.cps.gov.uk/news/press_statements/dpp_statement_on_tom_daley_case_and_social_media_prosecutions/index.html.

enforcing agencies to attend to such issues may deter people from accessing public services. e-Governance is inspired by freedom and trust which is ironically declining as the studies reveal. In the Philippines and Indonesia, there are grassroot groups emerging for the protection of online freedom. An Indonesian[10] online group Saura Blogger Indonesia (Indonesian Bloggers' Voice) raises awareness about threats to Internet freedom in Southeast Asian countries. Vietnam like Pakistan and China has been arresting and persecuting bloggers in a big way. In the Philippines, Senator Teofisto 'TG' D. Guingona III has placed a bill called 'Crowd Outsourcing Bill' for public comments. The senator is a great supporter of online freedom and, pursuant to this, demands greater public participation in the making of laws since it improves the quality of laws formulated[11] (Sifry 2012). Bangladesh is witnessing a full-fledged movement for the protection of Internet freedom which is growing along with the movement for press freedom or freedom of expression guaranteed by the Article 39 of the Constitution (VOICE 2012. Voices for interactive choice and empowerment, 30 September 2012). Pakistan has been witnessing a slow erosion of Internet freedom, but even in the midst of restrictions, the e-NGO Network for Internet freedom and rights to privacy is becoming active especially in the freedom city of Karachi. Bytes for all and RYSe (Reclaim Your Space) are already much ahead of making their visibility in public spaces as a voice of freedom over the net. Its support is gaining ground as their latest contribution to the movement is their working document released on 6 February 2013, titled 'Freedom of Expression and Net Freedom in the Manifestos of Political Parties in Pakistan: A Review of political parties manifestos for freedom of expression and internet freedom in the country'. This is a commendable movement even though the Pakistan judiciary since 2006 has been directing the government to keep tabs on Internet sites and block them for showing blasphemous content.[12] Barrister Amjad Malik, the applicant filed a petition under Article 184 (3) of the Constitution of Pakistan and prayed to the Chief Justice Iftikhar Muhammad Chaudhry for issuing necessary directives to the Pakistan Telecommunication Authority (PTA), the government and other concerned institutions of the country to block objectionable pages promoting blasphemy in the name of freedom of expression…protect the name of Prophet Mohammad and protect lives and liberties of mainstream Muslim population. The PTA then published requests for proposals for the 'deployment and operation of a national level URL Filtering and Blocking System'.[13] Much of this would follow the pattern of China's use of Golden Shield, the Great Fire Wall of China. This is to generate capacity to block fifty million websites in Pakistan. The Supreme Court imposed a blanket ban on all blogspots many times since 2006. There have been controversies about the YouTube as well which showed a controversial Dutch film *Fitna* and was asked to

[10] Goldman, Lisa (2012) Indonesian Grassroot Group promotes Internet freedom, Techin Asia, October 5.

[11] http://techpresident.com/news/23012/philippines-crowdsourcing-bill-filed-seeks-crowdsourced-improvements.

[12] 'Blogspot ban lifted in Pakistan',,(2006, 6 May) Wikinews.

[13] National ICT R&D Fund (March 2012). 'Request for Proposal'. National ICT R&D Fund.

block the content. When YouTube did not abide by the orders, the site was blocked.[14] Interestingly, this is a very frequent recurrence in Pakistan on the stated directives of the Supreme Court.

6.4 Ranking on Internet Freedom

The *Freedom on the Net 2012: A Global Assessment of Internet and Digital Media*,[15] a US-based research group, has studied selected indicators for ranking countries about their status on the issue of freedom of the Internet. The indicators selected for assessment included many commonly undertaken measures by governments like web blocking, shut down of the net services, pro-government blogging, arrests for anti-government bloggers to the formulation of new regulatory and punishment laws, physical attacks, custodial torture, deaths and disappearance of anti-government e-writers. Of the Asian countries only one country the Philippines was rated to be actually free at a score of 23. The list carries countries from every region, and the best score in freedom of the Internet which is that of Estonia at 10 is substantively far away from China at 85 and Iran at 90.

Out of the 'partly free' category, South Korea tops the list at 34 followed by India (39), Indonesia (42), Malaysia (43) and Sri Lanka (55). Out of the countries being studied in this book, only two countries Pakistan (63) and China (85) fall in the category of 'not free'. Both these 'not free' category countries and some 'partly free' category of countries like South Korea, India and Malaysia have been showing a decline in providing freedom of the Internet since 2011, whereas Indonesia shows improvement. Australia is one of the stable rank countries which comes in the first five best performing countries in the world where the standards on freedom over the Internet has benefitted universities, research institutions and businesses which manage misuse by installing their own local institutional arrangements for security of data. Such arrangements are able to filter locally and prevent cases of hacking.

6.5 Global Politics of the Internet Governance

The world is witnessing growing insecurities on two fronts: first, the USA at the steering wheel of the global Internet and secondly, data security, misuse and propaganda issues which hurt democracies and freedom of individuals. In September 2011, India, Brazil and South Africa held a Global Internet Governance Meet at Rio de Janeiro. They reaffirmed the Geneva Declaration and Tunis Agenda which were yet to be made operational. The need to bridge institutional gaps and fragmentation

[14] 'Pakistan blocks YouTube for "blasphemous" content: officials', (2008, 24 Feb)*Agence France-Presse (AFP)*.

[15] Kelly et al. (eds) (2012).

of policy and increased participation was discussed. They insisted for the constitution of a new regulatory body within the United Nations which would be an independent arbiter in conflicts and crisis. Later at the time of presentation of this proposal in the World Conference on International Telecommunications in Dubai in December 2012, Brazil and South Africa withdrew from the proposal, and more interestingly, India did not sign the communication treaty which was her own initiative.[16] An intense civil society movement erupted against the Indian government for restraining and trying to gain control over people's right to free communication. India succumbed to the demands of internet freedom protestors.

The objection of India and USA to the treaty was due to the fact that it contains a controversial Article 5B which is titled 'Unsolicited Bulk Electronic Communications'. The Article suggests governments' intrusiveness into people's privacy of content and communication:

> Member States should endeavor to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services. Member States are encouraged to cooperate in that sense.

This remarkable new world divide is taking place after the demise and now a rebirth of the Cold War on the issue of the Internet. The global Internet freedom has become a battle cry of Google as the Chinese government announced censorship laws. Even the Senate Judiciary Subcommittee discussed the business practices in China with concern.[17] India's proposed UN-Committee for Internet Related Policies (UN-CIRP) was slammed for moving away from multi-stakeholderism and instead opting for government-led regulation.

6.6 Who Governs the Internet?

The governance of Internet has so far been the responsibility and privilege of the USA. In the Universal Declaration of Human Rights in 1948, United Nations had made it amply clear that obstructions to information dissemination are an infringement of human rights. Article 19 of the Declaration is worded appropriately for the borderless world of Internet with an unquenchable thirst for information, even though the technology was nowhere in sight at that time:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

In view of the above objective and philosophy, the former International Telegraph Union (founded 1869) was changed to the International Telecommunication Union (1950) to work as a specialised agency of the United Nations on ICT.

[16] Bhardwaj, (2013, 17 Jan).

[17] CSPAN (2010, 2 March).

In its Resolution 73[18] adopted at Minneapolis meet of 1998, it resolved to set up a World Summit on Information Society. In 2001, the ITU Council decided to hold the World Summit on the Information Society in two phases, the first phase at Geneva 2003 and the second at Tunis 2005. WSIS further created the Internet Governance Forum to look into the specific needs of the Internet issues. The IGF was created in 2006 as an outcome of the Tunis Agenda of 'Enhanced Cooperation'. It draws its mandate from the Paragraph 72 of the Tunis Agenda which reads as follows:

Para 72. We ask the UN Secretary-General, in an open and inclusive process, to convene, by the second quarter of 2006, a meeting of the new forum for multi-stakeholder policy dialogue—called the Internet Governance Forum (IGF).

IGF is respected and accepted by member countries because it has been able to provide a democratic space for multi-stakeholders dialogue on Internet governance. It is neutral because it is part of the UN body and has been created by the World Summit on Information Society.

When the World Summit on Information Society (WSIS) held its meeting in 2003, the technical parameters of controls started changing to political surveillance, and in 2004 United Nations created a UN Information Commission Task force. In the 2005 Tunis Summit the Internet Governance Forum (IGF) emerged as a multi-stakeholder and amorphous agency of regulating the Internet. At this point the concern, anxieties and the fears of countries were coming to surface. Some countries wanted no regulation but others did demand a formal structure to regulate this meandering, free flowing powerful storm of energy lest the unworthy start harming the others. Control was found to be embedded in the nature of Internet technology which was different from a normal wireless or telephone technology. Being a 'network of networks', ICT passed information in channels called tubes, and if some start clogging these tubes with unsolicited and unwarranted information which leads to slowdown of transmission for others, then the Internet should have a structure of control just as one has it on other issues of governance.

The UN Commission on Science and Technology was allocated the responsibility of catching up with the other two incumbents in the area, i.e. WSIS and the IGF. Their second meeting at Rio de Janeiro in November 2007 kick-started a formal structure of governance for the Internet.

Internet Corporation for Assigned Names and Numbers (ICANN) is a nongovernment organisation based in Los Angeles, California, USA, since 1998. Presently it governs the Internet. Prior to ICANN, the Internet Assigned Numbers Authority

[18] Resolution 73 (Minneapolis, 1998) of the International Telecommunication Union (ITU) resolved to instruct the ITU Secretary-General to place the question of the holding of a World Summit on the Information Society (WSIS) on the agenda of the United Nations Administrative Committee on Coordination (ACC, now the United Nations System Chief Executive Board – CEB) and to report to the ITU governing body, the Council, on the results of that consultation. In his report to the 1999 session of the Council on that consultation, the Secretary-General indicated that the ACC had reacted positively and that a majority of other organisations and agencies had expressed interest in being associated with the preparation and holding of the Summit. It was decided that the Summit would be held under the high patronage of the UN Secretary-General, with ITU taking the lead role in preparations.

with the Department of Defense of the US government controlled the Domain Name Systems over the Internet. The ICANN was created to assume the responsibility under a United States Department of Commerce contract. The US government renewed the contract with ICANN in 2006 for the performance of the IANA functions. As the control of the Internet appeared more to be directed and influenced by the US government, the ICANN's relationship with the US government was clarified on 29 September 2006, when ICANN signed a new MOU with the US Department of Commerce. Thus the Department of Commerce retained the oversight responsibility, while the primary responsibility for policy formation in ICANN was delegated to three supporting organisations: Address Supporting Organization, Domain Name Supporting Organization and Protocol Supporting Organization. The Regional Internet Registries and the Internet Engineering Task Force agreed to serve as Address Supporting and Protocol Supporting Organizations, respectively. ICANN was assigned the DNS policy development besides the oversight and coordination responsibilities. Thus ICANN handles allocation of address blocks to the Regional Internet Registries, assignment of unique protocol numbers and management of DNS root zone files. However, whatever editing ICANN does to the allocation and removal of country code top-level domains or the root zone files have to be approved by the US Department of Commerce, and this includes the removal and addition of country code top-level domains.

As described in the previous chapters the Internet, emerged to spy and control defence establishments, especially during the Cold War era when Pentagon was its only use but currently, internet is the voice of freedom, of opportunities and of coming together. It has now become part of a democratic domain and its demise may destroy the strength and motivation which is strengthening democracy in every part of the world. Interestingly, Internet use initially was limited to serve the needs of the cold war. However, from here, the technology evolved to a potentially worldwide scale and interestingly became the liberator for societies. Now, 'it is a source of tremendous good and potentially dreadful evil, and we are only just beginning to witness its impact on the world stage' (Schmidt and Cohen 2013, p. 3).

There are multiple channels of the transfer of data. Every channel requires some regulatory arrangement. When a message is sent, there are the following channels which suggest regulatory point:

Sender of message > message > a channel > a receiver > a feedback mechanism

The sender is the starting point of Internet Protocol (IP) when addresses are allocated to the computer in use. IP address is an agreement on a standard for setting up packets and the system of address allocations. This is the first point which demands knowledge governance. The email message in digitised form is passed from here to channels where the Internet service providers (ISPs) or companies facilitate content transfer through bandwidths. Bandwidths are a 'battlefield for scarce resources' and have emerged as a sticky field of governance. One can have local access (LAN) through Ethernet local area networks or in the larger network of networks there are multiple tubes as provided by the ISPs such as that of optic fibre,

satellite or cable TV network. As Mathiason sums up in a definition of an Internet which he has given with Milton Mueller and Hans Klein after his insightful academic and practical involvement with a large number of development programmes across the world, 'The internet is the global data communication capability realized by the interconnection of public and private telecom networks using Internet Protocol (IP), Transmission Control Protocol (TCP) and the other protocols required to implement internet protocol networking on a global scale such as the Domain Name System (DNS) and Packet Routing Protocols'. (2009, p. 11). He further says that if government users including governments didn't have to worry about the content of messages or operability of the Internet technology, the management issue would have been much simpler and confined to the contours of operational technology provisions when an agreement on protocols and the network linkages to each other would have sufficed in regulatory arrangements.

From the rush for protocols to the management of networks to ensure a smooth flow of content, the issue need not have deepened into a cutthroat debate as it is going today[19] but for the draft treaty which is now waiting to be signed. From the domain of engineers, the Internet regulation is now in a wider field of international cold war politics[20] as well as a civil society movement which have demonstrated their might beyond what any governmental power can control. From policies which prevent discrimination of use to the telecom regulation, and encryption policy to the management of competition and investments, the field of regulations involving a benign-looking technology of the Internet is more complicated and visibly belligerent as other traditional battles on commercial products are. However there is a difference that the real control is beyond one country or a small group of countries to handle as there is no monopoly in Internet regulations and nations may have to generate and develop multi-stakeholder groups in a decentralised platform of governance where participation and access are open to all. The Google authors in an interview to Leslie D'Monte (Hindustan Times 2013, April 27, p. 25) remark that governments break Internet to stay on in power, and this should be seen in the light of 57% of world population still living under autocracies, or a large number of vulnerable population on the net being driven by religious autocratic cyber union like an Islamic web which suggests that some form of regulation is required but which should not be located with individual governments but should be a top-down international regulatory control.

In the present state of an evolving Internet regulations, the issue is much beyond the capacity of IT engineers to control or the norms of engineering architecture to regulate. It is now in the battle ground of politics and ballistic civil society where predatory and instinctive authority structures are gnawing to capture its control from people.

[19] Google vis-a-vis Indian government and others, Comcast etc.

[20] Nations are divided on two groups of Internet freedom group led by the USA and the Internet controlling group led by Russia and China.

6.7 Conclusion

The success of e-governance depends upon the ideal of universal accessibility of the Internet by people of all age groups. When governments provide online services, a large amount of private data of citizens go online and make them vulnerable to attacks both physical and net based. Thus while universal usage is the goal, data security and citizens' privacy is the new government responsibility. The policymakers in the developing countries are just now beginning to see the inherent dangers of Internet misuse when large-scale disruptions in cities and in personal and business lives can be caused by mischievous and hate content passed on emails or on social media sites. Governments have been readying to confront the issue and to enact rules to hold intermediaries responsible for user-generated content that is allegedly obscene, infringing, defamatory or otherwise illegal. Internet governance is becoming a concern for nations and international agencies such as the International Telecom Union (ITU), ICANN and the WSIS which have been occupied since 2003 to find a reasonable solution to the whole complicated problem. Terrestrial and cyber laws would be different. Whatsoever be the structure of such a cyber law, it indicates a paradigm shift in the understanding of the law. Yet by their fundamental fuzziness, 'governance' as well as the 'Internet' seem nowhere close to a standard clarification of 'Internet governance'.

Watergate Scandal in the USA led to the resignation of President Nixon, but it also highlighted that individual privacy had become more vulnerable with the coming of the electronic communication. The debate on control has been exacerbated by many incidents of administrative overstepping in resolving electronic communication conflicts across the world. In India during November 2012, Shaheen Dhada a young college student was arrested by the Mumbai Police for posting a message on Facebook to her friend Rinu Shrinivasan. The two girls were charged under Section 295A for hurting religious sentiments, apart from Section 66(a) of the Information Technology Act 2000. The British Royal Court judgement generates a better understanding of cyber offences in present times. Countries have also been ranked on the basis of selected indicators about their status on the issue of freedom of the Internet. Internet has provoked a new cyber cold war, and Asian countries are likely to play a very active political role in its resolution.

Bibliography

Bhardwaj SN (2013) Internet Governance Treaty Puts India in Uneasy Spot, Journalist

CSPAN (2010) Senate judiciary subcommittee hearing on Internet freedom. Accessed 26 Nov Indian Penal Code was enacted in 1927

Johnson DR, Post DG (1996) Law and borders: the rise of law in cyberspace. Stanford Law Rev 48:1367. SSRN: http://ssrn.com/abstract=535

Kelly S, Cook S, Truong M (eds) (2012) The freedom on the Net 2012: a global assessment of Internet and digital media. Freedom House, Washington DC. https://www.google.co.in/search?q=Advanced+SearchCongress%2C+Politics%2C+Booksand

Mathiason J (2009) Internet governance: the new frontier of global institutions. Routledge/Taylor and Francis, Oxon
Mumbai Mirror (2012) In Palghar, cops book 21 year old for FB post. Mumbai and The Hindu (19 Nov 2012). Mumbai shuts down due to fear not respect, New Delhi edition
Paul Chambers and Director of Public Prosecutions (2012) EWHC 2157 Case No: CO/2350/2011 Date: 27/07/2012
Public Law No. 93–579 (1974)
Rizk D (2011) New Indian Internet intermediary regulations pose serious threats to net users' Freedom of Expression. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2011/06/new-indian-internet-intermediary-regulations-pose. Accessed 3 Jun 2013
Schmidt E, Cohen J (2013) The new digital age: reshaping the future of people, nations and business. Alfred A. Knopf, Random House Publication, New York
Sifry M (2012) Philippines Crowdsourcing Bill Filed; Seeks Crowdsourced Improvements. Techpresident, 17 Oct
The Gazette of India (2009) The Information Technology(Amendment) Act 2008, New Delhi: Ministry of Law and Justice, GoI
The Google authors in an interview to Leslie D'Monte (Hindustan Times 2013, April 27, p 25)
The Privacy Act of 1974, 5 U.S.C. § 552a
VOICE (2012) Voices for interactive choice and empowerment, 30 Sept 2012

Websites Visited

https://www.eff.org/deeplinks/2011/06/new-indian-internet-intermediary-regulations-pose, on 3 June 2013.
SSRN: http://ssrn.com/abstract=535
https://www.google.co.in/search?q=Advanced+SearchCongress%2C+Politics%2C+Booksand