Interactions and Policy-Making:

Civil Society Perspectives on the Multistakeholder Internet Governance Process in India

Colin Agur
Ramesh Subramanian
Valerie Belair-Gagnon

INTERNET POLICY OBSERVATORY

CENTER FOR GLOBAL COMMUNICATION STUDIES

Interactions and Policy-Making: Civil Society Perspectives on the Multistakeholder Internet Governance Process in India[1]

Colin Agur
Yale University

Ramesh Subramanian
Quinnipiac University

Valerie Belair-Gagnon
Yale University

Abstract

This paper examines India's experience in developing national Internet policy by focusing on interactions among stakeholders in the Internet governance process. The paper begins by tracing the history of telecom policies in India along with the development of its IT sector as well as its civil society. It identifies the tensions, opportunities and threats that India has experienced in its Internet policy-making. It then reviews India's legislative and policy history from the IT Act of 2000 onward, noting the intentions and limitations of India's framework of Internet governance. A notable aspect of the paper involves a series of interviews with civil society stakeholders involved in India's Internet governance debates. These interviews are used to identify patterns of interaction among different stakeholders, and to understand the underlying power dynamics in India's policy-making process.

Keywords
India; Internet Governance; Internet Security; Policymaking; Policy Interactions

[1] The authors would like to thank Raphael Leung of Yale Law School for research assistance, and Laura Schwartz-Henderson, Briar Smith, and Ben Wagner at the IPO, Pranesh Prakash of the CIS, and the fellows of the Information Society Project at Yale Law School for their comments on our project.

Introduction

Today India stands at the threshold of becoming a major economic power and a leader among emerging economies. Its new stature has come with certain self-imposed responsibilities, the foremost of which is determining how to use its new economic standing to enhance development. It is estimated that more than 700 million Indian citizens live in rural villages lacking basic amenities such as electricity and running water. A second responsibility, that is almost as important (albeit with an external focus), is that of being a self-appointed spokesperson for other emerging economies on IT policies, especially Internet policies – both national and global. These new responsibilities are the subject of ongoing debates in India, involving the state, industry, and civil society. The debates seek answers to questions such as: "How to leverage ICTs, and notably the Internet, for national development?" "How to effectively use global networks to enhance commerce?" "What sort of Internet policies will ensure unfettered and equal access to all citizens?" "Who should be the stakeholders in designing such policy?" "How will free and open access balance against security?" and "How should global Internet policy be framed to make all of this a reality?"

Policy debates pertaining to Internet governance have assumed greater significance in recent years in India. The India Internet Governance Conference held on October 4-5 2012 (FICCI, 2012) addressed some of the above questions. It is notable that the conference was organized jointly by the Internet Society, the Federation of Indian Chambers of Commerce and Industry (FICCI), and the Indian Ministry of Communications and IT, attesting to emergent multistakeholderism. Much of the discussion thus far has focused on the current state of Internet governance, problems in the current structure, and changes needed to make the Internet an equitable and fair platform for the development of all countries – not just those that are technologically advanced.

In this project, we focus on Internet policy formulation in India in the context of Internet rights and principles, and within that, focus on security considerations. The context of reference is both national and global. We are interested in identifying the power brokers who set (or seek to set) Indian Internet policy, understanding their influences, both internal and external, and analyzing how national security considerations affect Internet policies. This approach enables us to discuss wider global and domestic Internet governance interactions and their impact on Indian policy-making that pertains to security issues.

Why study India? Motivations and Significance

The evolution of Internet policy formulation in India thus far is interesting for many reasons. To date, India's Internet policy has included elements of different modes of governance, and some of its positions have been contradictory. At times, the Indian government has advocated top-down or UN-based control, whereas at other times it has supported a multistakeholder approach

(Denardis, 2014). In September 2011, India, along with Brazil and South Africa, met at Rio de Janeiro (the "IBSA" Summit) and agreed on the idea of a United Nations organization that would deal with Internet governance issues. At the 66th session of the UN General Assembly (in September 2011), the Indian Prime Minister Manmohan Singh proposed the creation of a UN committee to manage the Internet, its standards bodies and policy organizations, treaties, and disputes. This attempt to shift Internet control to the UN was roundly opposed by the United States and the European Union. Recently, India has made an about-turn, joining the United States and the European Union by resisting a top-down governmental approach for global Internet governance. In 2012 at the World Conference on International Telecommunication (WCIT) in Dubai, India sided with the EU and US in support for the multistakeholder status quo. In doing so, India made clear its opposition to the approach proposed by some governments, including those of China, Iran, and Russia, which has called into question the multistakeholder model of Internet governance and advocated for more control by national governments. Since then, India has supported multistakeholderism in global meetings on Internet governance. Despite this support for multistakeholderism abroad, India's domestic record shows willingness by the government to act against the desires of internal and external stakeholders who favor an open Internet. Pro-free speech groups such as the Index on Censorship have scrutinized India's domestic record (Patry, 2013). Jyoti Panday of the Center for Internet and Society (CIS-India), a Bangalore based NGO, writes that 143 URLs have been blocked by the Department of Electronics and Information Technology in 2015 alone, stating that the procedure for blocking content remains opaque in India (Panday, 2015). Given this inconsistency in global and domestic actions, we ask: what power dynamics exert influence over Internet governance in India?

Several features of India's Internet make it significant for policymaking and for scholars studying global Internet governance. First, after a late start, India is now home to a large and rapidly growing Internet market. Although a relatively small percentage of citizens (15.1% in 2013) have access to the Internet, that nevertheless gives India the third largest number (185+ million) of users, after China and the United States (International Telecommunications Union, 2013). In the years to come, India's number of users will continue to grow dramatically. Cisco's Visual Networking Index estimates that the country's IP traffic will grow five-fold from 2013 to 2018, at a compound annual growth rate of 39%, reaching 3.6 exabytes per month in 2018, up from 680 petabytes per month in 2013 (Cisco Visual Networking Index, 2014).

Second, India's Internet infrastructure will expand and improve. Two major factors include the continued growth of mobile Internet in India (with most service offered by the private sector) and the National Optical Fibre Network (managed by the Bharat Broadband Network Ltd, a government-owned special purpose vehicle). These infrastructural improvements will allow for more users to access the Internet and for greater transmission speeds. What remains to be seen

is how effectively they will reduce the urban-rural divide in Internet access as well as help advance India's larger developmental goals.

Third, in part to encourage rural users, the Indian government is undertaking major efforts in e-governance. According to the Institute for Defense Studies and Analysis (IDSA), India's National e-governance Program (NeGP) is "one of the most ambitious in the world" (Institute for Defense Studies and Analysis, 2012: 20). The initiative seeks to bring more than 1,200 services online and encourage effective use of networks to relay data for communication purposes and for commercial transactions. The program involves major sectors such as Defense, Energy, Finance, Land Records, Law Enforcement, Public Essential Services, Security, Space, Telecommunications, Transport, and Utilities.

The growth of Indian Internet usage has often outpaced efforts to protect its infrastructure and users. One fundamental vulnerability is India's dependence on a few submarine cables that transmit substantial amounts of data. In 2008 and 2011, users in India suffered major loss of access as a result of cuts to cables under the Suez Canal and Persian Gulf.[2] In contrast to trans-Atlantic and trans-Pacific Internet traffic, data bound to or from India must pass through a handful of minimally protected cables, which (as happened 2008 and 2011) can be severed by underwater landslides or an errant ship's anchor.

Other, larger vulnerabilities to the Indian Internet involve malicious activity by users inside and outside the country. In recent years, an underground economy has flourished on India's Internet, thanks to low levels of computer security (Dharmakumar, 2011). Some estimates show that India is the world's third-largest generator of spam zombies and a major source of phishing hosts (Institute for Defense Studies and Analysis, 2012: 23-24). India's experience has also shown that its Internet infrastructure is unprepared to deal with sophisticated computer worms and other malware. Although Iranian nuclear infrastructure was the target of the 2010 Stuxnet attack, India suffered significant collateral damage, with more than 10,000 Indian computers, including 15 in critical infrastructure facilities, affected by the computer worm (Fitter, 2012). In addition, cyber-attacks and counterattacks by India and Pakistan (perpetrated by groups such as the Indian Cyber Army and Pakistan Cyber Army) have become routine events in recent years (Dilipraj, 2013). These have added impetus to arguments that national security considerations will have to be a big part of any Internet policy.

[2] For a map of the world's major submarine cables and the 2008 cable cuts, see: The Guardian (2008). "The Internet's Undersea World." Available at: http://image.guardian.co.uk/sys-images/Technology/Pix/pictures/2008/02/01/SeaCableHi.jpg

Research-Questions and Methods

Our objective is to explain transformations in Internet governance in India in terms of interactions among global and domestic players, civil society, private interests, and technological infrastructure. We explore the interactions that produce Internet policy in India, emphasizing the relationship between security and Internet rights and principles. We study inside and outside interactions – including those among civil society, political and regulatory bodies, Internet service providers (ISPs), content providers, transnational governance bodies and users – and these actors' influence on global meetings such as the IGF. Civil society in India, despite its nascent state, is beginning to play an important role as an arbiter of Internet policy debates, especially on the issue of Internet rights and freedoms accorded to citizens. Therefore, we focus our interviews primarily on civil society players and, to a lesser extent, on representatives from the industry and academic communities. The historical discussion and governmental views have been excerpted from published policy papers and reports.

Our analysis thus keeps in mind historical developments that have shaped Internet policy, modes of governance, and civil society. In recent years, India's government has realized both the popularity and disruptive potential of the Internet, especially social media. Accordingly it has pursued a mixed set of policies intended to balance technological development with social harmony. We consider the complex set of interactions that have shaped policy, the ways that macro shifts in culture, politics, economics, and institutions have changed the nature and scale of these interactions, and the implications that these interactions have for future policy frameworks. We believe that these interactions have important ramifications for India's Internet policy as well as for other emerging economies (particularly heterogeneous societies) and, more broadly, for global governance of a shared resource. Accordingly, our research focuses on these interactions by examining three questions: (1) What tensions among state, technology, and market forces shape India's Internet policy? (2) What effects do external influences such as global associations, multilateral meetings, and global political dynamics have on shaping India's Internet policy? (3) What are the trends resulting from this combination of existing policies and global forces?

In what follows, we present the results of our study in three parts. In the first part, we present a historical analysis of the political economy of telecommunications in India after independence. We discuss how India gradually recognized the importance of the Internet and the country's attempts to increase its presence in international forums pertaining to Internet governance. We then trace the evolution of civil society in India and discuss multistakeholderism in an Indian context.

In the second part, we discuss our study of legislation and policy documents that tell the early story of India's domestic Internet policies and the country's role in global Internet governance. Multiple laws and policies have shaped security and Internet freedom-related debates in India (Prakash, 2013). We have focused on India's Information Technology Act (2000) in its original and amended forms, and the notifications and charter of the Computer Emergency Response-in India (CERT-In). In our analysis of these documents, we seek to historically construct Internet governance since 2008, focusing on security and Internet rights and principles issues. Together, these documents show the growth and evolution of India's domestic Internet policies, and the relationship between wider political events, especially the Mumbai terrorist attacks of 2006, and government policies.

In the third part, we discuss the results of a set of semi-structured interviews with civil society stakeholders. Our sample was purposive, since we selected interviewees who are directly involved with the issues of security and Internet rights. We asked respondents to discuss (a) background information on their role in global/national Internet governance, security and Internet rights and principles, (b) their motivations for change in security and Internet rights as well as their principles and potential motivation for changes since 2008, and (c) examples of changes in Internet governance and the role of civil society in making those changes. The rationale behind those questions was to analyze the social dynamics that have shaped global and national Internet governance since 2008.

Each of these three components contributes to the paper's overriding goal: to understand the complex interactions that shape Internet governance in India. By studying the history and political economy of telecommunications in India, we can understand how rapidly and profoundly India's telecommunications sector has grown since the 1990s, and the type of challenges that have faced policymakers. And by studying India's Internet policies, we can understand both the factors - technical, economic and political - that influenced policies, as well as the ways that early legislation on a nascent Internet had effects later on. Last, by speaking to civil society groups involved in the policymaking process, we are able to understand the nature of multistakeholderism in India, the shifting power dynamics, and what is at stake in Internet governance interactions. The paper is thus more than an analysis of Internet policy itself; it is an effort to understand the origins of a policy framework and the implications of that framework for privacy, security, freedom of speech, and democratic participation.

1. Telecommunications in Post-Independence India: A Brief History

To fully understand India's Internet governance debates and stances, we need to understand the development of communication technologies and policies in India throughout the last three decades. From its independence in 1947 until economic liberalization (which tentatively started

in 1984) in 1991, India followed the mantra of socialistic self-reliance. Central planning, large state-run enterprises, and stringent import restrictions on technology characterized this period. Economic and technological growth was choked by post-colonial policies built from a deep mistrust of the capitalist, colonial system (Subramanian, 2006). This had a major effect in limiting the country's telecommunications development. From 1947 until 1985, Indian telecommunications was controlled by the state monopoly PTT (Posts, Telegraphs and Telecommunications Department). Research was virtually non-existent and telephones were considered a privilege rather than a right. Public opinion and interests were not worthy of consideration. A graphic example of this callous attitude is a 1984 exchange in the Indian Parliament between an opposition member and C.M. Stephen, Minister of Communications in Indira Gandhi's government. When the opposition member questioned the poor quality of telecommunications service provided by the government monopoly, the Minister,

> …replied in a lordly manner that telephones were a luxury in a developing country, that the government had no obligation to provide them or improve the service, and that if the honorable member didn't like his telephone, he could return it, because there was an eight-year-long waiting list of people to get landlines. (Tharoor, 2007)

Relief arrived in 1991 when the Indian government, faced with a severe balance of payments crisis, was forced to borrow from the IMF, with attendant conditions. One of the conditions required the liberalization of its economy, and the Narasimha Rao government was forced to adhere. In the years afterward, economic liberalization resulted in impressive GDP growth rates of around 9% per year and has remained strong even after the global economic downturn in 2008 (Subramanian, 2011a). The growth has been spearheaded by the IT and software industry. The Global Technology Services sector has successfully weathered global uncertainties, and its revenues for the financial year 2015 is expected to cross the landmark figure of 150 billion USD. This sector represented almost 9.5% of India's GDP in 2014, and has played a substantial role in India's development over the last two decades (NASSCOM, 2015).

In 1998, the Indian government realized that it needed to take drastic steps to enhance the country's IT infrastructure and take advantage of the then-nascent Internet. Prime Minister Atal Behari Vajpayee set up a multistakeholder National Task Force on IT and Software Development whose goal was to develop ideas and strategies to make India an IT superpower and one of the world's largest generators and exporters of software in ten years (i.e. 2008). The task force members consisted of government officials and select representatives from the IT industry and a couple of educational institutions. No general members of the public or NGOs were involved (NIC, 1998). The task force collected ideas and suggestions that became the basis for an "Information

Technology Action Plan." This plan eventually led to the passage of the IT Act of 2000. The IT Act of 2000 followed the Model Law on Electronic Commerce adopted by the UN Commission on International Trade Law (UNCITRAL), which provides legal recognition of electronic documents and digital signatures, addresses offenses, contraventions, and cybercrimes – all of which were pertinent to Internet-based commerce. The Act covers cyber offenses committed against individuals (e.g. distribution of obscene material, harassment, hacking, transmitting viruses, and network trespassing), organizations (e.g. possessing unauthorized information, cyber-terrorism, and distribution of pirated software), and society at large (e.g. pornography, trafficking, and corrupting young people). The law applied to any computer user in India, as well as to persons in other countries who commit crimes using computers or networks located within India (IT Act of 2000).

India and Internet Governance

Recognizing the geopolitical importance of the Internet, the Indian state has for the last decade and a half sought to increase its presence in international forums on Internet governance. The government as well as civil society (represented by NGOs) participated in the WSIS in Geneva (2003) and Tunis (2005). At WSIS-Tunis, the original agenda – to address the digital divide and human rights issues among nation states – was quickly overshadowed by calls for a more democratic way to frame Internet policies and governance issues through an UN-based Internet Governance Forum. Paragraph 72 of the Tunis Agenda mandated the UN Secretary-General to convene a forum to conduct multistakeholder policy discussions (P.J. Singh, 2008). The process was initiated through the creation of the Working Group for Internet Governance (WGIG), which eventually led to the creation of the Internet Governance Forum (IGF). The Indian government supported this, and Indian NGOs such as IT for Change played a major role in the initial formation of the IGF. Parminder Singh of IT for Change and Nitin Desai, an Indian career bureaucrat, initially took on the role of special advisors to the IGF Chair.

Over the years since the inception of the IGF, the Indian government's position has generally coincided with the position of many Indian NGOs, especially their suspicion of the Internet Corporation for Assigned Names and Numbers (ICANN). The Indian government and Indian NGOs held a shared suspicion that ICANN, which governed the operational aspects of the Internet, remains under the influence of the US government. There was belief in the notion that ICANN, being a US-registered corporation, was beholden to the US Department of Commerce and US laws, and thus was not an appropriate neutral entity that could be trusted with the governance the global Internet (Joshi, 2013; Kaul, 2014). Indian NGOs were resentful of US attempts to categorize the role of ICANN as purely "esoteric," technical and research-oriented in nature, focused on smooth functioning of the Internet (and the stability, security, and robustness of the infrastructure), and the insinuation that developing countries would be better off by just

"consuming" the Internet and focusing on building applications to suit their development agenda. A research paper from an Indian NGO at the first IGF conference focused primarily on how Internet governance should be moved away from ICANN, on the grounds that it was under the control of US government and business interests, and "rich country clubs" such as the Organization of Economic Cooperation and Development (OECD) (P. J. Singh, 2008). The Indian government made several statements to the effect that while it was generally satisfied with the status-quo regarding Internet operations, it preferred that ICANN's work be performed by an UN-based organization that had multistakeholder membership, which could then bring the views and development imperatives of the (UN) member states to the table. This is evident from Prime Minister Manmohan Singh's address at the 66th UN General Council meeting in September 2011 favoring moving ICANN under the authority of the UN, an idea that resulted from the IBSA meeting of 2011 (as noted in an earlier section). India's position was firmly opposed by the EU, the US, and other OECD members. The US justified its position on the basis that such a move would lead to more governmental control, which would result in censorship of the Internet in several countries with poor human rights records.

Internet Free Speech and Security Considerations

While India has a record as a strong democracy that protects free expression in its law and constitution,[3] its record on Internet free speech has nevertheless been uneven. As early as 2003, India designated the Department of Telecommunications as the single authority to order blocks on certain sites and issued a notification on July 7, 2003, stating that "websites promoting hate content, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography and violent sex can reasonably be blocked" (Ministry of Communication and Information Technology, 2003a). A 2007 report by the OpenNet Initiative[4] tested several Internet service providers in India and found evidence of government filtering of sites whose contents related to national unity or national security (OpenNet, 2007). India also has a history of overt censorship and blocking of sites. Examples include: the blocking of all Yahoo Groups in September 2003 after Yahoo refused to block access to the group Kynhun, which promoted the secession of Meghalaya from India; the blocking of the extremist web site www.hinduunity.org in April 2004; and the blocking of seventeen web sites, including blog sites, after the 2006 Mumbai bombings (Sengupta, 2006).

[3] Article 19 of the Indian Constitution protects freedom of speech and expression. Article 19. (1)(a) states that "All citizens shall have the right to freedom of speech and expression." Available at: http://lawmin.nic.in.

[4] The OpenNet Initiative is a collaborative project, involving several major Internet research centers, to monitor and report surveillance activity by national governments.

Government attempts to filter and block sites have continued despite changes in governments and prime ministers. The media and some civil society activists have usually met such initiatives with strong resistance. These groups argue that the Indian government has played a double game: on the one hand, the government was pushing back on what it considered the overt influence on the Internet by US tech companies and the US government. On the other hand, the government was attempting to control free speech on the Internet. Over time, NGOs began to realize that with respect to Internet governance, the Indian government was more interested in promoting multilateral agreements (at a country-country level) rather than multistakeholder agreements, which would include a variety of domestic stakeholders (including civil society).

The impact of the 2008 Mumbai terrorist attacks effectively nullified growing opposition to the government's approach. In the weeks that followed, Indian lawmakers hurriedly passed the Amendment to the IT Act of 2000 with little debate or opposition from civil society (Subramanian, 2011). The Amended Act (under sections 66-69) listed a host of actions that would be deemed computer-based crimes. That same year, speaking at the Internet Governance Forum (IGF) in Hyderabad, Jainder Singh, Secretary of the Department of Information Technology, described the Internet as both "a vehicle" to enhance communication and "a target of criminal minds" (Moody, 2011). NGOs such as the Centre for Internet and Society (CIS-India) and the People's Union for Civil Liberties (PUCL) opposed these moves, saying that the Amendments were an attack on Freedom of Speech and amounted to censorship (Prakash, 2012). In the ensuing years, India has experienced increased debate on whether unfettered Internet access poses a threat to security, and on the kind of governance that would provide the right balance of access and security. Much of this debate plays out in the media and through opinions and position papers from civil society NGOs. However, the number of NGOs involved in the Internet governance debate is still extremely small, and the influence they exert is uneven. Sivasubramanian Muthuswamy, President of the Internet Society (ISOC) of India – Chennai Chapter, stated in an interview that the number of NGOs involved in Internet governance and Internet policy issues numbered less than ten, and that there was not a significant and consistent civil society-led movement on Internet issues in India at present. In looking at the role of civil society in influencing Indian Internet policy issues it is useful to examine the history and evolution of civil society in India.

The Evolution of Civil Society in India

Political scientists studying the development of state and civil society in India have noted significant differences between this growth in India and similar developments in the West. In the case of Western Europe, the state and civil society developed both independently and parallel to each other over a long period, during which both the state and civil society became stronger, more efficient, and independent of each other. The Indian case, as noted by Henrik Berglund (2009), has been different. Both in the pre-colonial and colonial period, the state in India always

co-existed with traditional religious power structures. The British colonizers realized this and divided the population according to religion, and ruled by cultivating and co-opting religious elites. This led to a strengthening of religious identity as well as a strengthening of the power held by religious elites (Belair-Gagnon et al., 2014; Freitag, 1989, p. 109).

The beginnings of contemporary Indian civil society can be traced to the early years of the 20th century and the emergence of the Indian National Congress. Under the Indian National Congress, intellectuals united to form a cohesive unit opposed to British rule, bringing together Indians of different faiths and social strata. The Indian National Congress, while fundamentally focused on freedom from British rule, also facilitated within its ambit movements such as the women's movement, labor movement, and other social reform movements. For many of these movements, the political sphere as well as the economic sphere served as their raison d'être, as restrictive British laws and taxes had suffocated the domestic industry and damaged prospects for economic development.

In this nascent Indian civil society, many of the bourgeoisie who participated in the movement were also the same people who were under British employment, as managers, lawyers, and teachers. Thus, an uncomfortable and unspoken nexus between the state and civil society existed in the early days of India's civil society. The first Indian trade union, the All India Trade Union Congress (AITUC) formed in 1920, was an early effort to organize a section of Indian society outside of the influence of the state and capital owners. It became an important instrument for enhancing the awareness of the labor class, and also served as a "rudimentary civil society" (Berglund, 2009).

After independence, the Indian government set up a Planning Commission that established five-year plans for the country's political and economic development. Thus, even after independence, the economy was dominated by the state. During the 1960s, however, the country's mostly agricultural economy suffered several setbacks due to droughts, a resulting food crisis, and wars with China and Pakistan in 1962 and 1965, respectively. These crises helped vitalize the labor movement, which was joined by both urban and rural groups in a series of protests.

Contemporary Indian civil society had its beginnings during the "Emergency" (from 1975 to 1977) when Prime Minister Indira Gandhi declared that escalating civil and political unrest had created dangerous destabilization. Upon her advice, the President of India declared an emergency, which gave the Prime Minister the power to rule by decree, subverting many fundamental rights of Indian citizens. Civil, political and legal rights were severely curtailed. The Emergency became the basis for the rise of numerous protest movements and a reemergence of civil society groups in the late 1970s and 1980s. These groups comprised a cross-section of civilians including workers,

academics, students, and peasants. Other groups that formed during this period and focused on specific agendas, such as the Hindu nationalists, environmental groups, and women's rights organizations, gained strength during this period.

Another boost for civil society came with the Eighth Five Year Plan (1992-1997), which allocated funds for NGOs. The state realized that NGOs were better and more successful at reaching and providing many types of required services to the population. Some commentators such as Lucy Dubochet believe that this was the start of the "NGOization" of civil society in India, and resulted in the dramatic growth of NGOs operating in India (Dubochet, 2012). As NGOs grew in number and size, they came to depend increasingly on external agencies for funding. Some of these agencies were Indian, while many were from outside of India. Significant state funding also strengthened the dependent relationship between the state and civil society.

Amir Ali notes another important aspect of the evolution of Indian civil society, which he refers to as the separation of the public and private sphere (Ali, 2001). The British found it expedient to rule through representative governance by separating the religious groups (mainly Hindu and Muslim) and dealing only with representatives of these groups. Two types of laws were created – one for the public sphere (i.e. governance, land and commercial dealings, etc.) and one strictly for the private sphere (i.e. separate personal laws for Muslims and Hindus governing family issues, marital relationships, inheritance, codes of conduct, etc.). This system has persisted over time, through the nationalist movement, up to the present. Thus, there is a common view that civil society does not address the concerns of all communities equally. Minority concerns (i.e. non-Hindu, women, and lower castes) are not adequately represented, and minority opinions are not easily accepted. Today's NGOs, while purporting to represent multiple stakeholders, may actually, and at times inadvertently, be addressing only the concerns of the majority populations (or the elites) that they represent.

This historiography of Indian civil society provides a context to the presence, activities, and perceived role and effectiveness of civil society in India. This history is especially useful in understanding civil society's values, views on multistakeholderism, and its relationships with the state as well as industry. This also sets up the context for a discussion on civil society's interactions with government and industry with regard to the Internet governance process in India.

Multistakeholderism in an Indian Context

"Multistakeholderism" in Internet governance generally refers to interactions across technical developers, private sector providers, civil society, and governments as opposed to top-down

governance.[5] For example, ICANN's stated mission is to: "bring together the primary stakeholders such as businesses, civil society, governments, research institutions and non-government organizations to cooperate and participate in the dialogue, decision making and implementation of solutions to common problems or goals" (ICANN, 2014).

Until recently, the term 'multistakeholderism' in the Indian context has mostly meant some ad hoc combination of representation from the state, corporate interests (i.e. industry), civil society (mostly well-established NGOs), and academics. In practice, this idea of multistakeholderism can be seen in the composition of the National Task Force on IT and Software Development set up by Prime Minister Atal Behari Vajpayee in 1998. As noted earlier, this task force primarily consisted of government officials and select representatives from the IT industry and a couple of educational institutions—members of the public or people from NGOs were not included (NIC, 1998).

Frequently, interviewees highlighted the social and economic context in which the Internet has developed in India. Parminder Singh of *IT for Change* noted that issues in Internet policy were different in India when compared to the West. Singh agreed that concepts such as free speech, free trade, and an uncensored Internet (concepts championed by the West) were laudable. However, he also commented that the West has become somewhat "mono-focused" (i.e. having a singular approach) on these issues. This, he felt, did not leave much scope for different interpretations and prioritizations of policy in other nations, especially in developing countries.

Samir Saran and William Poff-Webster (2014) reach a similar conclusion. In their analysis, the services expected by the poorest citizens used to be *bijli, sadak, and paani* (electricity, roads, and water). However, these needs are now rapidly changing to *bijli, sadak, paani,* and *Internet.* The original needs remain, but they have been augmented by the need for Internet. NGOs such as *IT for Change, CIS-India,* and *The Centre for Communication Governance* are advocating for more participation in Internet policy discussions by various segments of the population, making the process much more multi-stakeholder oriented.

When it comes to the question of Internet rights and principles, there has been tension in the relationship among the multistakeholder approach, national security interests, and Internet rights. This has been debated in India frequently since the terrorist attack of 2008. The debate has focused on surveillance, privacy, and government access to individual online data (discussed in an earlier section). While these debates are not new in the global context, as noted earlier,

[5] India's UN-CIRP (Committee for Internet-related Policies) proposal was rejected by several countries including the US. The countries that rejected the proposal claimed that this committee would pass control of the Internet to the UN.

Indian civil society's involvement in Internet policies has been relatively recent (within the last decade). Civil society has become vocal in stating its opinions on domestic issues such as surveillance of Indian citizens and censorship, as well as net neutrality.

The Indian government has reacted to civil society advocacy by attempting to frame Internet policies. While acknowledging these moves, many of our civil society interviewees noted that government efforts at engagement have not resulted in civil society gaining greater influence in the formation of Internet policies. At the same time, it has also become clear that the Indian government has started to play a more active role in international Internet governance discussions. The government has been gradually verbalizing its own views and seeking multilateral alliances with a few other countries.

Typically, Indian NGOs involved are funded by a variety of sources: charitable trusts located in India; the state; UN agencies such as UNDP, UNICEF and UNESCO; and foreign aid agencies such as the IDRC (Canada), Sigrid Rausing Trust (UK), Kusuma Trust (UK) and others. Given the varied funding sources, it is prudent to examine if and how donors might influence the NGOs' views, especially with respect to multistakeholderism. Our interviewees were specifically asked about this. Their overall responses indicate that the source of funding did not significantly influence their objectives as facilitators of greater multistakeholder participation in the Internet policy-making process. One interviewee specifically noted that over the last few years, there has been a profusion of international funding for Internet Governance to NGOs. However, some NGOs have balked at such funding, because, as noted earlier, of the narrow and "mono-focused" interests of the funding agencies. Parminder Singh noted that such a straight-jacket approach would not work in India, with its plurality of interests. With respect to government monies influencing NGO interests, Singh noted that government funding often came from states that were run by different political parties that were not aligned to the central government, and were often focused on their own narrow interests, such as rural education and empowerment of women, etc. Thus, their influence on other related policies such as Internet Governance was minimal if not non-existent.

It is not surprising that civil society organizations argue that they choose their own destinies and are not the proxies of benefactors (domestic or foreign). In fairness to these organizations, they must raise money from somewhere, and the growth in funding for civil society indicates several trends. One trend is that Indian civil society has reached a level of sophistication that international donors have taken notice. A related trend is that India has become a crucial market in online commerce and other aspects of Internet usage and, as a result, the expertise Indian civil society organizations offer is essential in discussions about privacy and security (and a host of other issues). More broadly, the growth in funding for Indian civil society organizations allows us

to reflect on multistakeholder Internet governance. Multistakeholderism is complex process, with alliances that cross borders, involve different types of organizations, and link countries rich and poor, large and small. Increasingly, these alliances defy the tidy categories of 'government', 'industry', and 'civil society' that have framed much of the thinking and discussion about multistakeholder governance.

This section has discussed the growth of India's telecommunication sector and the involvement of civil society organizations in the Internet governance process. This history is prologue for the next section, which examines the legislation and policy documents pertaining to Indian Internet policy. In that section, we show the ways that civil society became involved in the Internet governance process, first as opponents to certain provisions in the IT Act and later as sources of expertise, proponents of certain policies, and active players in a process that has expanded to include a wider range of stakeholders.

2. Internet Legislation and Policy in India

The starting point for this policy history is the Information Technology Act (2000), the first comprehensive piece of legislation in India on e-commerce and cybercrimes. The Act provides for "the legal recognition of transactions carried out by ... alternatives to paper-based methods of communication and storage of information" (Indian Parliament, 2000). The IT Act's main actions included legally recognizing electronic records and communications, creating a regulation framework for Certification Authorities (i.e. the entities that issue digital certificates), and cyber contraventions (i.e. acts that violate cyber laws prevailing in a jurisdiction, but not considered criminal - thus they may lead to civil prosecutions, but not criminal prosecutions) (Blythe, 2006). The Indian government's decision to pass the IT Act followed initiatives by the United Nations and by other Asian governments. In their assessment of the law five years after its passage, Basu and Jones write: "The Act is based on the Model Law on E-Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) and no doubt was prompted by the passing of such legislation by neighboring countries, such as Singapore and Malaysia" (Basu and Jones, 2005: 210).

The IT Act of 2000 was a far-reaching document, meant to cover a wide range of activities, and written with the expectation that the Internet would grow and evolve. In subsequent years the Act has faced criticism for being too expansive and for undermining privacy and free speech (Holder and Grimes, 2006). For an example of its expansiveness, see Section 2 (1) (o), which defines data in very broad terms by including all kinds of personal, banking, financial, confidential health, and insurance related data (Dugal, 2008). The only safeguard that the IT Act of 2000 provides to data is with respect to the penalty in cases of breach or unlawful activity (Bharadwaj, 2010).

Three years after passing the IT Act, the Indian government formalized its process for blocking websites. In important "Notifications" in 2003 and 2004, the government established the Computer Emergency Response-in India (CERT-In) and the procedure for blocking of websites. According to the Ministry of Telecommunications notification dated February 27, 2003:

> India (CERT-In) shall be the single authority for issue of instructions in the context of blocking of websites. CERT-In, after verifying the authenticity of the complaint and after satisfying that action of blocking of website is absolutely essential, shall instruct Department of Telecommunications (DOT) - (LR Cell) to block the website. DOT, under whose control the Internet Service Providers (ISPs) are functioning will ensure the blocking of websites and inform CERT-In accordingly. (Ministry of Communications and Information Technology, 2003b)

CERT-In subsequently established a charter and released statistics on the organization's efforts. The charter provides a national mandate for the agency:

> The purpose of CERT-In is to become the nation's most trusted referral agency of the Indian community for responding to computer security incidents as and when they occur; the CERT-In will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents. (CERT-In, 2015)

In 2010, CERT-In published statistics showing that the majority of computer security incidents handled (61%) concerned "website compromise and malware propagation," vastly eclipsing the second-largest component, virus/malicious code at 27% of incidents (CERT-In, 2010).

In the years since its creation, CERT-In has expanded and clarified its role as the national coordinating body for government blocking of websites. But its role has limits: According to Lallie, CERT-In "generally does not get involved in digital forensic investigation" (Lallie, 2012: 3). However, after the Mumbai attacks, this limitation was laid bare. It became clear that there was no specific agency charged with conducting digital forensic investigations, nor was such an entity legally sanctioned or able to identify and recognize an impending attack.

In 2008, the IT Act was substantially amended to give the government new powers of investigation. Some of these changes focused on digital forensics. For example, previously, Section 78 of the Act had stated that the investigation and recording of a statement of offences

committed under the act must be carried out by "a police officer not below the rank of Deputy Superintendent of Police" (Indian Parliament, 2000). But as Lallie notes:

> A Deputy Superintendent of Police … is often not available at smaller police stations which in turn limits the locations and opportunities at which a cybercrime could be reported. Section 78 was revised in the amendment such that an inspector was now able to receive and investigate an act of cybercrime. The act is therefore less restrictive and potentially allows cybercrimes (in theory at least) to be reported and investigated by any police station. (Lallie, 2012: 7)

While the amended IT Act extended into cyber law, it did not address several important issues, including: payment, copyright, media convergence, cyber-squatting, and questions of jurisdiction. As Internet usage in India continues to grow, the Act's limitations will require further amendments. Today, the dissemination of computer viruses, hacking, and denial of service attacks are major problems for corporate houses, service providers, and users (Ahmad, 2010).

In addition to large-scale legislative changes, the Indian government has also undertaken ad hoc policies in response to specific concerns and threats. In April 2011, new laws extended the scope of Internet surveillance to cybercafés through "Cyber Cafes Rules." Under these rules, Indian mobile phone users must register their names and provide a copy of government-issued ID to activate SIM cards. Additionally, Internet service providers are required to grant government authorities access to users' data (Acharya, 2011). In June 2013, *The Hindu* revealed significant domestic surveillance and an absence of a legal or procedural framework to protect privacy online (S. Singh, 2013). Section 69 of the IT Act gives the state surveillance powers in the interest of national security or "friendly relations with foreign states" (Indian Parliament, 2008). In these initiatives, the Indian government has attempted a difficult balancing act. Kapil Sibal, the Minister of Communications and Information Technology, has stated that India believes in "complete freedom of the Internet" but at the same time "needs to acknowledge that along with cyber freedoms come cyber gangsters, and the state and its citizens need to be protected from them" (Kaul, 2013).

With Indian internet governance still evolving, civil society actors have stepped up, offering technical and legal expertise with the goal to influence government policy. Indian NGOs have also stepped up their presence in national and international forums on Internet policy, such as the India Internet Governance Conference (New Delhi, 2012) and several IGF meetings. Some have joined international coalitions such as The Internet Rights and Principles Dynamic Coalition (IRPDC), an open network at the IGF. This coalition promotes "an equal right to access and use a secure and open Internet" (Internet Rights and Principles Dynamic Coalition, 2015). A recent example of such NGO participation is the Internet Democracy Project's participation in the

"Global Multi-Stakeholder Collaboration for Achieving a Safe, Secure, and Tolerant Cyberspace," a meeting held on the sidelines of the IGF in Bali on October 21, 2013. Several NGOs were also present at the NETmundial Global Multistakeholder Meeting on the Future of Internet Governance, held April 23-24, 2014 in São Paulo, Brazil.

At domestic and especially international fora, Indian civil society organizations have become active participants in discussions related to Internet governance. In this new activism, we can identify a set of capacities as well as limitations on the change that civil society can actualize practice. To date, civil society organizations have played roles as experts on technical and legal details, and as representatives for a range of interests beyond those of the government and major commercial players. Civil society organizations have established their place in a process of consultation that governments have generally respected, if at times half-heartedly. In the case of India, while civil society organizations have not always been happy with government policies on the Internet (or, more broadly, telecommunications), these organizations have been able to scrutinize these policies and have, in some cases managed to effect changes in policy. But as civil society organizations themselves admit, their powers are limited in the present multistakeholder process. While they can offer expertise, promote transparency, scrutinize legislation, and criticize action; civil society organizations cannot set a legislative agenda (as governments can) and they do not represent a large economic sector (as the tech industry does). As a result, civil society organizations must deploy their limited resources in ways that make the most impact. The third section of this paper examines the interactions civil society organizations undertake in promoting security and Internet rights.

3. Interactions and Influences in Policymaking

We interviewed members of civil society organizations involved in India's Internet governance debates. In our interviews with civil society players, we asked interviewees to discuss their experiences dealing with security issues, and in participating in discussions (in India and at global meetings) on how to protect security and Internet rights. Our analysis of the interviews revealed four common themes: (1) a desire for a broader understanding of 'security' in policy, (2) encouragement of greater emphasis on users' rights, (3) worries about sovereignty and lobbying by US technology giants, and (4) suggestions that the government improve technical knowledge among policymakers and judges. In this section, we discuss each of these themes in turn.

Understanding 'Security' Policy

Several interviewees criticized government definitions of security as too narrow and overly focused on government priorities (at the expense of users' rights). Rishab Bailey, Legal Consultant to the Society for Knowledge Commons, stated: "We see security as a broad issue, not just the specific issue like 'is your data being stolen?' or 'the fight against terrorism.' So we would look at

it as a matter of economic independence or dependence, looking at security of user data." Also calling for a broadening of the concept of security was Anja Kovacs, Director of the Internet Democracy Project. She argued that:

> Our starting point was that security is an innate human need, and for us to use the Internet therefore we have to first feel secure. But that if you turn security on its head like that – if you think that is the starting point of security – then a strong defense of the rights to freedom of expression and privacy should be at the heart of any security policy.

These and other interviewees emphasized a common theme: that good security policy can coexist with and even reinforce free speech. As Part I of this paper discussed, many Indian civil society organizations have criticized policies that have limited free speech in the name of making the Internet a safe place (e.g. the 2008 amendments to the IT Act of 2000, especially sections 66-69). Some organizations have pointed out that, instead of the blunt 'pro-security' approach of the 2008 Amendments (and, since then, the government blocking websites that threaten to stir up local unrest), there are a nimbler set of options governments could deploy. By censoring websites and punishing their creators, the government leaves intact the underlying conditions (poverty, inequality, poor governance, corruption, violence) that prompted the offending online behavior. Left unchecked, these underlying conditions can lead not just to future offensive behavior online, but future insecurity as well. By taking this larger view - that social and economic justice can lead to a more secure and safe Internet - governments can end the false binary of 'security vs. free speech' in Internet policymaking. With this type of argument, Indian civil society organizations have sought to make 'security' a broader and more socially inclusive concept, and one that goes beyond the day-to-day security of specific sites or networks.

User Rights

Many interviewees expressed frustration about the status of users' rights, which they saw primarily as something to be protected from actions by governments, industry, and other actors. Interviewees argued that users' rights needed greater attention and legal status. Rishab Bailey spoke for many interviewees when he said:

> At the national level, we believe it is essential that we have fair legislation within the limits of the Constitution to protect the rights of our citizens. This is required urgently, which is why the Marco Civil[6] is an excellent example for our government

[6] The "Marco Civil da Internet" is a civil-rights based framework for the Internet which was signed into law by Brazil's President, Dilma Rousseff, in April 2014, during the NETmundial meeting in Sao Paulo, Brazil. Brazilian activists had long fought for this legislation, which has been dubbed the "Internet Constitution." The law seeks to

> in terms of having a rights--based framework domestically, and I think we need one internationally as well.

Similarly, focusing on the need to curb excessive surveillance, Chinmayi Arun, Research Director at the Centre for Communication Governance at the National Law University, advocated policies that are rooted in traditional methods for tracking non-cybercrimes. She stated:

> The main problem I see with the existent work on cybersecurity is that many assume the premise that the only way to identify cybercrime is through surveillance... The way to track cybercrime is the same way you track ordinary crime – patience in understanding these networks, infiltrating them and earn trust, then map out the organization. And so all of that can be done without use of many surveillance tools, because cyber criminals are usually pretty sophisticated online.

In general, there is preference for developing civil-rights based frameworks that would protect user rights in the fight against cyber criminals.

"Users' rights" as noted by Arun refers to users' privacy rights, and the right not to be surveilled, while protecting the right to information and free speech (and thus the right from censorship). While this seems to be a fairly general and well-understood concept, it has particular relevance to Indian users, as the Indian government has, time and again, resorted to covert and overt surveillance, curbs on free speech (with the accompanying threat of arrests), and censorship, as noted in many instances above. These have been accomplished through various laws that have at times been pushed through without much discussion or explanation leading to interviewees' preference for developing civil-rights based frameworks.

National Sovereignty and Foreign Influences

The stakeholders we interviewed were concerned about national sovereignty. Several mentioned the Snowden disclosures and fears of surveillance by US and other countries' intelligence agencies. A representative quote comes from Arun:

> Unlike China, which has essentially cut itself off from the Internet, India has very much hooked onto the Internet. We need the ability to not just protect ourselves

reinforce the protection of fundamental freedoms in the digital age, and was developed through a participatory process. However, as the EFF notes, the Marco Civil did not pass "without getting caught in the traditional horse-trading of the legislative process, which resulted in several concessions. One of the most damaging concessions, fiercely opposed by digital rights activists, was a data retention mandate that compels the collection and storage of connections logs of any innocent individual." (Pinho and Rodriguez, 2015).

> but also to influence global discourse. While we have always pushed our government to use open-source solutions, this has a higher stake post the Snowden revelations.

Interviewees also raised the related issue of the power exercised by foreign technology giants (especially Google and Facebook) on the Indian government. These companies often enjoy a place on the Indian government's delegation at major conferences, such as the World Conference on Information Technology (WCIT), but Indian companies rarely enjoy that kind of proximity to power. As one anonymous interviewee[7] stated: "Even organizations that are supposed to represent corporate interests, whether it is FICCI[8] or NASSCOM,[9] by and large tend to represent the certain interests of big American companies." Some stakeholders we interviewed argued that – fair or not – as a developing country, India struggles for legitimacy in the industrialized world. As an interviewee explained:

> I was frustrated that globally there was this very simple discourse of: the US was the harbor of Internet freedom... and on the other hand, you had supposedly oppressive states which were always in the developing world. And sometimes it made it sound like all developing countries are authoritarian. So it was a very simplistic and polarized debate. We felt the concerns of non-authoritarian developing countries don't get taken seriously.

Frequently, governments face pressure from international corporations with something to lose if new legislation strengthens user rights, or champions local and national alternatives to existing dominant players. As Arun argued:

> The international big content platforms – the Googles, the Facebooks, the Yahoos – are the ones who push back. Initially, their stance had been that since they are not Indian companies, [and] especially since content decisions are not made in India, they are not obligated to fully follow Indian law. I don't know how long they will be able to maintain this position because it is a fairly large market. [Moreover] the government has been talking recently about data localization. But typically it is the multinational corporations that have pushed back and have argued from time to time.

[7] We have included the names of only those interviewees who agreed to have their names released. Others have been kept anonymous in this paper.
[8] The Federation of Indian Chambers of Commerce and Industry is an association of business organizations in India.
[9] The National Association of Software and Services Companies is a trade association in India's IT sector.

It should be noted here that foreign companies operating in India are obliged to follow Indian law. However, foreign companies can use technical loopholes to circumvent such laws. For example, when the mobile telephone vendor Blackberry was ordered by the Indian government to provide access to user information, Blackberry claimed that since its secure servers were located in Canada, it could not comply with the order. In contrast, an Indian telecom executive we interviewed noted that his company generally acceded to government requests.

In interviews, members of civil society seemed to have mixed feelings about sovereignty and foreign influences. On the one hand, several were vocal in their opposition to foreign surveillance and foreign dominance of the Internet economy. On the other hand, some of these same civil society organizations heralded the benefits of international tech companies in opposing (what our interviewees saw as) bad domestic policies. In several cases, it was through the international multistakeholder process that Indian civil society organizations gained enough prominence to attract the attention of the Indian government. In their complicated relationship with sovereignty, Indian civil society organizations have internalized some of the tensions between 'domestic' and 'global' forces in Internet governance.

Technical Knowledge Deficit

Among civil society actors, there is increasing recognition that legislators and judges need to better understand communication technology. As Mishi Choudhary of the Software Freedom Law Centre noted,

> …[India's] democratically elected legislators do not understand [the Internet]. Even at the judicial level… the side that explains technology better is the side that wins, because judges don't understand technology. So this is an issue that intertwines technology, law, and policy. And this affects and impacts lots of people in business, tech and beyond.

This lack of understanding of technical issues sometimes results in conflicting policies. For example, this is apparent in some of the Indian government's attempts at regulating the encryption standards used for common Internet communications. Kovaks noted that according to Indian regulation, the government has set the "ridiculously low" upper limit of 40-bit key length encryption for users (without seeking government permission). This means that, "if you use https on your Gmail, you are, strictly speaking, breaking the law" (since https on Gmail uses higher bit encryption key-lengths). According to Kovacs, the government specifies low-level encryption standards for private communications between citizens "because they want to be able to access everybody's data."

There are also other contradictions. As noted by Salman Waris, the Securities and Exchange Board of India (SEBI) prescribes a 64-bit/128-bit encryption for standard network security and mandates the use of encryption technology for security, reliability and confidentiality of data. SEBI recommends use of secured socket layer security, preferably with 128-bit encryption, for securities trading over a mobile phone or a wireless application platform. Thus two different encryption standards are being suggested by SEBI and the Reserve Bank, respectively. This is likely to cause more confusion in the conduct of Internet based commerce in India.

In their efforts to shape policy outcomes, different stakeholders try to influence public opinion through print and digital media and by capitalizing on particular public events. In practice, the influence that they exert is amplified when the debate on the issues in question is also taken up at a global level. Problems arise when globally debated issues move to the forefront of national policy-making bodies, to the detriment of other issues that are important from a local point of view. As Arun notes:

> When nation-states are talking to each other, the conversation is often only about security. While security is important, balance in creating procedures such that we do not violate anybody's rights in the quest for security is also important. I do not think that has been achieved. So our role is to do whatever we can to make sure that is achieved. For example, [concerning] security policy ... the parties discussing were not really very mindful of building human rights into it, and making sure the procedures are rights- protective.

Arun also noted that push-back by local industry against policies that have human rights impacts is negligible. One could conjecture that this could be because of the deep nexus that continues to exist between Indian industry and the governmental agencies – remnants of the pre-liberalization years when the government completely controlled industry, and when the industry could only move forward by establishing personal connections or through rent-seeking behavior.

The growth of the Internet in India has created new power dynamics, with the government at the center of a national debate about security and rights. In that debate, the arrival of civil society has created new alliances based on a complex alignment of interests. What has emerged is not simply a process of actors coming together in a concert; instead it is a process of actors funding, shaping, interacting with, and seeking to influence each other in a fluid and interactive form of governance. In our interviews, we uncovered several aspects of the debate about security and rights. Part of the debate is about definitions and scope (e.g. what constitutes 'security'); part of the debate is about priorities (e.g. users' rights); part of the debate is about what should be national and what should be global; and part of the debate is about technical literacy and the

role of expertise in policymaking. In these debates about security and Internet rights, we see that governments have retained their roles as agenda-setters, but have been joined in the policymaking process by a range of actors. The result is a set of policymaking interactions that cross borders, involve alliances among different types of participants, and transcend the boundary between 'domestic' and 'global'.

Conclusion

Today, the multistakeholder model of Internet policy-making is beset with challenges. One such challenge is that the various interests involved engage in communication and advocacy efforts that cross national borders. More often than not, the interests themselves are shaped by external as well as internal events and movements. Social and cultural aspects also come into play. In addition, the structural features of the Internet itself constrain regulation.

In our analysis of legislation and policy documents and in our interviews with stakeholders, we sought to understand the interactions and power dynamics at work in India's Internet governance. Internet policy-making in India is a complex process involving a mix of stakeholders and discussions at the local, national, and global levels. History also plays a major part in how the interactions, as well as tensions, have evolved. While global discussions of Internet governance have been years in the making, national differences (in laws, practices, user culture, and vulnerabilities) continue to persist. By focusing on national governance of a global technology, we have learned about the changing power relations that exist in the global multistakeholder model, as well as the ways in which discussions at the national and global levels influence each other and shape policy outcomes.

Our research shows that the state uses civil society to the extent that it suits the state, and more importantly, in order to keep up the *appearance* of inclusivity. Yet that does not mean that civil society is completely powerless. Working in coordination with the free press, civil society has, time and again, brought to the forefront issues such as privacy, freedom of expression and access to information in the context of the state's need for security. This became very apparent in the March 24, 2015 Indian Supreme Court ruling which declared Section 66A of the Information Technology Act unconstitutional (Sriram, 2015). Section 66A banned statements made on the Internet that could cause "annoyance," "inconvenience," "enmity, hatred or ill-will." Application of this law had resulted in, among others: the arrests of two college girls who had made a Facebook posting questioning the government-ordered shutdown in Mumbai due to the death of a popular politician; and the arrest of a citizen in Southern India for his Twitter post accusing a politician of corruption. Shreya Singhal, a law student, challenged the law's constitutionality; she and was supported in her lawsuit by NGOs such as the People's Union of Civil Liberty (PUCL), the Center for Internet and Society, and the India and the Centre for Communication Governance

of the National Law School. The Supreme Court judgment was a major victory for freedom of expression in India, as well as for civil society.

In the game of shifting loyalties and issue-based policy making, industry has occasionally sided with civil society in calling for the above-mentioned issues. On other occasions, however, the state has held more power over the industry in the way security has been implemented. Overall, it is fair to say that while the number of civil society organizations in India is plentiful, only a handful of these engage in serious and persistent actions focusing on Internet governance issues. These are almost always indigenous organizations that nonetheless are acutely aware of external affairs, issues, and challenges.

In fact, the Indian public as well as the Indian government have a deep-seated mistrust of foreign organizations and abhor foreign interference—a deep rooted fear that stems India's colonial past. Indian civil society organizations periodically benefit from foreign assistance, but do not blindly accept directions from abroad, unless it suits their local interests. These organizations have endured numerous shifts in fortune from occasionally antagonistic governments, to corporations and vice versa. However, India's civil society has been surprisingly effective in bringing issues to the forefront of Indian society. In this they have been aided by another democratic and (mostly) neutral institution—the Fourth Estate. The press and the media have managed to remain free of overt government and corporate interference, and in the end, this makes the difference as to how effective or ineffective the civil society has been on shaping Internet governance in India.

Bibliography

Acharya, Bhairav (2011). Comments on the Information Technology Guidelines for Cyber Cafe Rules. Available at: http://cis-india.org/internet-governance/blog/comments-on-the-it-guidelines-for-cyber-cafe-rules-2011.

Ahmad, Tabrez (2010). Copyright Infringement In Cyberspace And Network Security: A Threat To E-Commerce. *IUP Journal Of Cyber Law* 9.1/2 (2010): 17-24.

Ali, A. (2001, June 30). Evolution of Public Sphere in India. *Economic and Political Weekly*, 2419–2425.

Belair-Gagnon, Valerie, Smeeta Mishra and Colin Agur (2014). Reconstructing the Indian Public Sphere: Newswork and Social Media in the Delhi Gang Rape Case. *Journalism: Theory, Practice & Criticism*, Vol. 15, No. 8, pp. 1059-75

Berglund, H. (2009). Civil Society in India: democratic space or the extension of elite domination. Working Paper, Stockholm, Stockholm University. Available at: http://www.socant.su.se/polopoly_fs/1.129706.1364285702!/menu/standard/file/berglund_civil_society_in_india_oct_2009.pdf

Basu, Subhajit and Richard Jones (2005). Indian Information And Technology Act 2000: Review Of The Regulatory Powers Under The Act. *International Review Of Law, Computers & Technology* 19.2.

Bharadwaj, Kritika (2010). How Safe Is This Shore? - Data Protection And BPOs In India. 27 *John Marshall Journal of Computer and Information Law*.

Blythe, Stephen E. (2006). Critique of India's Information Technology Act and Recommendations for Improvement. 34 *Syracuse J. Int'l L. & Com*.

Cisco Visual Networking Index (2014). VNI Forecast Highlights, Filtered by Country. Available at: www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html.

Computer Emergency Response-in India (2015). Charter. Available at: http://www.cert-in.org.in/.

Computer Emergency Response-in India (2010). Statistical Brochure. Available at: http://www.cert-in.org.in/.

Dara, Rishabh (2011). Intermediary Liability in India: Chilling Effects on Free Expression on the Internet. Center for Internet and Society, Bangalore. Available at: http://cisindia.org/internet-governance/intermediary-liability-in-india.pdf.

DeNardis, Laura (2014). *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Dharmakumar, Rohin (2011). Hackers' Heaven. *Forbes*, Sept 19, 2011. Available at: http://forbesindia.com/printcontent/28462.

Dilipraj, E. (2013). Cyber Warfare and National Security – An Analysis of Incidents between India and Pakistan. *Air Power Journal*, *8*(3). Available at: https://www.academia.edu/7534559/CYBER_WARFARE_AND_NATIONAL_SECURITY_-_AN_ANALYSIS_OF_INCIDENTS_BETWEEN_INDIA_AND_PAKISTAN.

Dubochet, Lucy (2011). The Changing Role of Civil Society in Middle-Income Country: A Case Study from India. Oxfam India. Available at: http://www.oxfamindia.org/sites/default/files/XI%20The%20Changing%20Role%20of%20Civil%20Society%20in%20a%20Middle-Income%20Country.pdf.

Dubochet, L. (2012). Civil Society in a Middle-Income Country: Evolutions and Challenges in India, *Journal of International Development*, 24(6), 714–727.

Dugal, Pavan (2008). Legal Issues Relating to Outsourcing in India. 36 *International Journal of Legal Information*.

Fitter, Pierre Mario (2012). Stuxnet Attack Wakes India up to Threat of Critical Infrastructure. *India Today*, Sept. 5, 2012. Available at: http://indiatoday.intoday.in/story/stuxnet-cyber-war-critical-infrastructure-of-india-ntro/1/216107.html.

Freitag, S. B. (1989). *Collective Action and Community: Public Arenas and the Emergence of Communalism in North India*. Berkeley and Los Angeles: University of California Press.

The Guardian (2008). The Internet's Undersea World. Available at: http://image.guardian.co.uk/sys-images/Technology/Pix/pictures/2008/02/01/SeaCableHi.jpg.

Holder, James T. and David E. Grimes (2006). Government Regulated Data Privacy: The Challenge for Global Outsourcers. 38 *Georgetown Journal International Law*, 695-712.

Internet Corporation for Assigned Names and Numbers (ICANN) (2014). Multistakeholder Model. ICANN Wiki. Available at: http://icannwiki.com/index.php/Multistakeholder_Model.
Indian Parliament (2000). Information Technology Act.

Indian Parliament (2008). Information Technology Act, Amendment, 2008. Available at: http://cca.gov.in/cca/sites/default/files/files/itact-amendments2009.pdf.

Institute for Defense Studies and Analysis (2012). *Task Force Report: India's Cyber Security Challenge*.

International Telecommunications Union (2013). Time Series Statistics on Individuals Using the Internet, 2000-2013. Available at: www.itu.int/en/ITU-D/Statistics.

Internet Rights and Principles Dynamic Coalition (2015). About. Available at: http://internetrightsandprinciples.org/site.

Joshi, S. (2013, December 7). India to push for freeing Internet from U.S. control, *The Hindu*. Retrieved March 21, 2014. Available at: http://www.thehindu.com/sci-tech/technology/internet/india-to-push-for-freeing-internet-from-us-control/article5434095.ece

Kaul, Mahima (2013). India Challenges Cyber Governance and Security. X Index, October 25, 2013. Available at: http://www.indexoncensorship.org/2013/10/india-challenges-cyber-governance-cyber-security.

Kaul, Mahima (2014). Global Internet Governance: India's search for a new paradigm. ORF Issue Brief#74, August 2014. Available at: http://www.globalpolicyjournal.com/sites/default/files/ORF%20Issue%20Brief%2074%20Mahima%20Kaul_0.pdf

Lallie, Harjinder Singh (2012). An Overview of the Digital Forensic Investigation Infrastructure of India. *Digital Investigation* 9.1: 3-7.

Ministry of Communications and Information Technology (2003a). Ministerial Order on Blocking of Websites. Dated July 7, 2003.

Ministry of Communications and Information Technology (2003b). Notification no. G.S.R.181(E), dated February 27, 2003. Available at: http://www.naavi.org/cl_editorial_06/notification_270203_blocking.htm.

Moody, Glyn (2011). India Wants UN Body To Run The Internet: Would That Be Such A Bad Thing? *Techdirt*, November 2, 2011. Available at: http://www.techdirt.com/articles/20111102/04561716601/india-wants-un-body-to-run-internet-would-that-be-such-bad-thing.shtml%20accessed%20on%202%20September%202013.

NASSCOM. (2015). India IT-BPM Overview | NASSCOM. Retrieved April 17, 2015, from http://www.nasscom.in/indian-itbpo-industry

National Taskforce on IT and Software Development (NIC) (1998). Membership. Available at: http://it-taskforce.nic.in/member.htm.

OpenNet Initiative (2007). Research. Available at: http://opennet.net/research.

Panday, Jyoti (2015). DeitY says 143 URLs have been Blocked in 2015; Procedure for Blocking Content Remains Opaque and in Urgent Need of Transparency Measures. April 29, 2015. Available at: http://cis-india.org/internet-governance/blog/deity-says-143-urls-blocked-in-2015

Patry, Melody (2013). India: Digital freedom under threat? India's role in global internet debates. X Index, November 21, 2013. Available at: http://www.indexoncensorship.org/2013/11/india-online-report-freedom-expression-digital-freedom-5.

Pinho, L., & Rodriguez, K. (2015, February 25). Marco Civil Da Internet: The Devil in the Detail. Electronic Frontier Foundation. Retrieved April 30, 2015. Available at: https://www.eff.org/deeplinks/2015/02/marco-civil-devil-detail

Prakash, Prakash (2012). Indian Government's Submission to ITU, Centre for Internet and Society. Available at: http://cis-india.org/internet-governance/blog/indian-govts-submission-to-itu.

Prakash, Pranesh (2013). How Surveillance Works in India. India Ink blog, *The New York Times*, July 10, 2013. Available at: http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0.

Raboy, Marc et al. (2010). *Digital Solidarities, Communication Policy and Multi-stakeholder Global Governance*. London: Peter Lang.

Sai Manish (2011). India is a Sitting Duck in the Cyber Battlefield. *Tehelka*, Vol. 8, Issue 47, Nov 26, 2011. Available online: http://archive.tehelka.com/story_main51.asp?filename=Ne261111India.asp.

Saran, Samir and William Poff-Webster (2014). Re-Imagining Multistakeholderism: Challenges for Internet Governance. Observer Research Foundation, *Issue Brief 84* (December 2014). Available at: http://orfonline.org/cms/export/orfonline/modules/issuebrief/attachments/orf_issue_brief_84_1417758397679.pdf.

Sengupta, S. (2006). India Blocks Blogs in Wake of Mumbai Bombings. *The New York Times*, July 18, 2006. Available at: http://www.nytimes.com/2006/07/18/world/asia/18cnd-india.html?gwt=pay.

Singh, P. J. (2008, June). A Development Agenda for Internet Governance – Call for a "Framework Convention on the Internet" | IT For Change Position Paper. Available at: http://intgovforum.org/Substantive_1st_IGF/A%20Development%20Agenda%20for%20IG%20-%20ITfC.pdf

Singh, Shalini (2013). India's Surveillance Project May be as Lethal as PRISM. *The Hindu*, June 21, 2013. Available at: http://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece.

Sriram, J. (2015, March 25). SC strikes down "draconian" Section 66A, *The Hindu*. Retrieved May 1, 2015. Available at: http://www.thehindu.com/news/national/supreme-court-strikes-down-section-66-a-of-the-it-act-finds-it-unconstitutional/article7027375.ece

Subramanian, Ramesh (2006). India and Information Technology: An Historical and Critical Perspective. *Journal of Global Information Technology Managemen*t, Vol. 9, No. 4.

Subramanian, Ramesh (2008). The (Continuing) Evolution of India's Telecom Policy. *Communications of the International Information Management Association*, Vol. 8, No. 3.

Subramanian, Ramesh (2011). The Growth of Global Internet Censorship and Circumvention – A Survey. *Communications of the Association for Information Systems*, Vol. 11, No. 2. Available at: http://www.iima.org/index.php?option=com_phocadownload&view=category&download=331:

the-growth-of-global-internet-censorship-and-circumvention-a-survey&id=56:2011-volume-11-issue-2&Itemid=68.

Subramanian, R. (2011). ICTs and Access to Knowledge in Rural India: A Comparative Study of Two Models of Deployment. In *Access to Knowledge in India* (pp. 109-147). Bloomsbury Academic Publishing.

Tharoor, S. (2007, November 7). The Elephant, the Tiger, and the Cell Phone: Reflections on India, the Emerging 21st-Century Power. Carnegie Council. Available at: http://www.carnegiecouncil.org/studio/multimedia/20071107/index.html

Waris, S. (2013). *Indian Lawyer 250: A Guide to the Leading Business Law Firms in India*. June 6, 2013. Available at: http://indianlawyer250.com/features/article/81/encryption-india/.

Interviews

Name	Interview Date
Mishi Choudhury	April 25, 2014
Rishab Bailey	May 12, 2014
Anja Kovacs	May 22, 2014
Chinmayi Arun	Mar 23, 2014
K. Shankar	August 28, 2014
Parminder Jeet Singh	February 23, 2015
Sivasubramanian Muthuswamy	March 13, 2015
Vinayak Godse	May 16, 2015

Other interviewees wished to remain anonymous