SECURITY, INTERNET RIGHTS AND PRINCIPLES: POWER SHIFTS AND IMPLICATIONS FOR INTERNET POLICY-MAKING IN INDIA

Colin Agur, Valerie Belair-Gagnon, and Ramesh Subramanian

The authors are undertaking a research project about internet policy in India as part of the CGCS’s Internet Policy Observatory.

Of the South Asian countries, India alone has a record as a strong democracy that protects free expression in its law and constitution. Nevertheless, its record on internet free speech has been uneven, with a history of overt censorship and blocking of sites. A 2007 report by the OpenNet Initiative tested several internet service providers (ISPs) in India and found evidence of government filtering for sites whose contents related to national unity or national security. Other incidents include: the blocking of all Yahoo Groups in September 2003 after Yahoo refused to block access to a 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.

Government attempts to filter and block sites have usually encountered strong resistance from activists and the media. However, in December 2008, in the weeks following the Mumbai terrorist attacks, Indian lawmakers hurriedly passed an amendment to the IT Act of 2000 with little debate or opposition. 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 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.” Nongovernmental organizations (NGOs) such as the Center for Internet and Society (CIS-India) and the People’s Union for Civil Liberties (PUCL) opposed these moves,
stating that the Amendments were an attack on freedom of speech and amounted to censorship.\textsuperscript{5}

Over the past few years, India has experienced increased debate on whether unfettered internet access poses a threat to security and what kind of internet governance would provide the right balance between access and security.

Internationally, the Indian government has sought to carve out a middle position on internet governance. In September 2011, India, along with Brazil and South Africa, met at Rio de Janeiro (the “IBSA” Summit) and agreed to the idea of a United Nations organization that would deal with internet governance issues. At the 66th session of the UN General Assembly, Indian Prime Minister Manmohan Singh proposed the creation of a UN committee to manage the internet, its standards bodies, policy organizations, treaties, and disputes. While Jainder Singh’s remarks suggest a top-down approach to internet governance, the Prime Minister’s proposal refers to a commitment to multistakeholderism in India’s internet policy.\textsuperscript{6} The multistakeholder internet governance model refers to interactions among technical developers, private sector providers, civil society, and governments as opposed to top-down governance which emphasizes command, control and hierarchy.\textsuperscript{7} Nevertheless, there is not a single unified understanding of internet governance in India.

**Global Stakeholders and Tensions in Internet Governance**

Internet governance remains a broad term used in various contexts including regulation, coordination of technical standards, development, and policy-making. The definition of the multistakeholder internet governance model has been contested by different groups.\textsuperscript{8} For the Internet Corporation for Assigned Names and Numbers (ICANN), such a model:

\begin{quote}
\begin{em}
aims 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. A stakeholder refers to an individual, group or organization that has a direct or indirect interest or stake in a particular organization; that is, a given action has the ability to influence the organization’s actions, decisions and policies to achieve results.\textsuperscript{9}
\end{em}
\end{quote}

The relationship between the multistakeholder approach, national security interests and internet rights has been debated in India since 2008.\textsuperscript{10} This debate has focused on surveillance, privacy and government access to individual online data.

For this project, we restrict our scope to global and national internet policy research focused on security within the context of internet rights and principles. This approach enables us to discuss wider global and domestic internet governance interactions and their impact on policy-making that pertains to security issues. Our research focuses on these interactions and asks three
fundamental 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?

Global and national interactions in policy-making have important ramifications for India’s internet policy, for other emerging economies (particularly heterogeneous societies) and, more broadly, for global governance of a shared resource. Over time, India’s internet policy has included elements of different modes of governance, which appear seemingly inconsistent and sometimes contradictory. India recently joined the United States and the European Union by resisting a top-down governmental approach for global internet governance. At the 2012 World Conference on International Telecommunication (WCIT) in Dubai, India sided with the EU and US and again promoted the multistakeholder status quo. In doing so, India highlighted both its support of global multistakeholderism and its opposition to approaches proposed by governments including China, Iran and Russia, which have questioned the multistakeholder model and advocated for more internet governance control by national governments.

More recently, India has taken more contrary stances. An internal note prepared after the meeting of the Sub-Committee on International Cooperation on Cyber Security held under the National Security Council Secretariat (NSCS) states that all internet traffic originating from or landing in India should be stored in India. Further, the note also seems to favor a multilateral, rather than multistakeholder, approach to internet governance, stating that “…a small unrepresentative group of certain individuals, supported by vested interests, appear to have arrogated themselves the right to present certain views in discussions relating to Internet Governance.” While this internal note does not carry official status, it nevertheless illustrates tensions within the Indian government’s position. India’s domestic record, however, shows the government’s willingness to act against the desires of other stakeholders who favor an open internet. Groups such as the Index on Censorship and the Center for Internet and Society have scrutinized India’s domestic policies on internet governance. This inconsistency in global and domestic actions raises the question: What power dynamics exert influence over internet governance in India?

**Surveillance and Internet Freedom: Who Holds Power?**

Multiple laws, policies and actors have shaped security and internet freedom-related debates in India. In April 2011, new laws extended the scope of internet surveillance to cybercafes through “Cyber Cafes Rules.” Currently, Indian mobile phone users must register their names and provide a copy of government-issued ID to activate SIM cards. Additionally, ISPs are required to grant government authorities access to users’ data. In June 2013, The Hindu revealed significant domestic surveillance and an absence of a legal or procedural
framework to protect privacy. Section 69 of the IT Act gives the state surveillance powers in the interest of national security or “friendly relations with foreign states.”

Multiple actors have also been at the forefront of global and domestic internet policy dialogues. These actors include civil society (including advocates of free speech such as the Center for Internet and Society, Internet Democracy Project and IT for Change), global internet governance institutions (Internet Society (India), Internet Governance Forum (IGF) and ICANN), private companies and their interests (Bharti Airtel, Reliance Communications, Bathy Enterprises, FICCI), academics and politicians. These groups compete and seek to promote various sets of global and domestic norms. For example, 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.” Meanwhile, on October 21, 2013 at the Bali a meeting entitled “Global Multi-Stakeholder Collaboration for Achieving a Safe, Secure, and Tolerant Cyberspace,” Anja Kovacs from the Internet Democracy Project, an Indian NGO, advocated for internet rights. Globally, organizations such as the Internet Rights and Principles Dynamic Coalition (IRPDC), an open network at the IGF and a global player in the internet governance debate, promoted “an equal right to access and use a secure and open Internet.” There is not one singular message coming from India, and sometimes even individual actors contradict themselves.

This multifaceted dialogue reveals the complexity and challenge of national internet policy-making. The primacy of national governments is reflected in their ability to censor and control sites they find offensive or politically inconvenient. At the same time, the authority of national governments is subject to technological and commercial forces. As Monroe E. Price writes, “laws are made at the national level, but norms and pressures increasingly come from the global.” Our preliminary analysis shows that interactions among disparate actors are at the core of changes in power in internet governance in India, an area of study that requires more attention from social scientists. This, however, does not answer the question: How do information environments such as described above affect internet law and policy?

**Global Internet Policy Logic as a Framework for Analysis**

One of the challenges of the multi-stakeholder model is that the groups involved engage in communication and advocacy efforts that cross national borders. Additionally, the social and structural aspects of the internet make the internet’s regulation complex and labor-intensive. Considering the current logic of internet governance in relation to security, internet rights and principles in India, relevant questions to ask are: Who holds power? What are the interactions among these global and domestic dynamics over time? How do information environments affect law and policy? These questions reflect what Monroe Price refers to as a “market of loyalties”
in which “large-scale competitors for power, in a shuffle for allegiances, often use the regulation of communications to organize a cartel of imagery and identity among themselves” that “dominates the world’s consciousness.” Applied to internet governance and the case of security and internet rights and principles, we ask: To what extent do actors’ inherent loyalties shape global and domestic internet policy? And does the regulatory scheme change when there is a shift in power or when the current regulatory scheme is unable to sustain the status quo?

Our research aims to explain transformations in internet governance in terms of interactions among global and domestic players, civil society, private interests, technological infrastructure, and identity. 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 influences – including political parties, regulatory bodies, think tanks, ISPs, content providers, and users – their interactions, and their influence on global meetings. Our project is a history of policy interactions in an important national context since 2008, with implications for other national contexts.
References


2 The authors contributed equally to this post and are listed alphabetically by last name. We thank Laura Schwartz-Henderson and Briar Smith at the IPO, Pranesh Prakash of the CIS, as well as the fellows of the Information Society Project at Yale Law School for their comments on our project.

3 Article 19 of the Indian Constitution protects freedom of speech and expression. Article 19. (1)(a) ‘All citizens shall have the right to freedom of speech and expression’ http://lawmin.nic.in


7 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.


Featured Photo Credit: Some rights reserved by Sanyam Bahga