CONNECTING THE DOTS: INTERACTIONS IN INTERNET RIGHTS AND SECURITY 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. In this post, Agur et al describe perspectives on India’s internet governance sphere from members of Indian civil society.

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, internet service providers (ISPs), content providers, transnational and national users – their interactions, and their influence on global meetings. Our project is a history since 2008 of policy interactions in an important national context that has implications for other national contexts as well.

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?
To answer these questions we used an inductive approach. During the spring and summer of 2014, we conducted a series of in-depth, semi-structured interviews with stakeholders in India’s internet governance debate. These stakeholders included political parties, regulatory bodies, think tanks, ISPs, content providers, and users. We also conducted textual analysis of laws and policy documents. Our sample was purposive, since we selected interviewees who are directly involved with the issues of security and internet rights. In our interviews, we asked stakeholders to discuss their experiences dealing with these security issues and participating in discussions, both in India and at global meetings, on how to protect security and internet rights.

**Challenges for Indian Internet Governance**

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 fast-growing internet market. Although a relatively small percentage of citizens (15.1% in 2013) have access to the internet, India still has the third largest number (185+ million) of users, after China and the United States. 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.

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.

Third, in part to encourage rural internet users, the Indian government will undertake major efforts in establishing e-governance mechanisms. 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.” That 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 of the vulnerabilities lies in 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 the Persian Gulf. 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 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. Some estimates show that India is the world’s third-largest generator of spam zombies and a major source of phishing hosts. India 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.

In this research we seek to understand the ways in which the Indian government develops policy to manage these, and other, security concerns; the type and extent of internet rights the Indian government has promoted; and the role different stakeholders have in this process.

**Perspectives from Civil Society**

In the first phase of our project we interviewed members of civil society organizations involved in India’s internet governance debates. Our analysis of the interviews revealed five common themes: (1) a desire for a broader understanding of ‘security’ in policy, (2) worries about sovereignty (in light of the Snowden disclosures), (3) eagerness for more accountability in lobbying by US technology giants, (4) encouragement of greater emphasis on users’ rights, and (5) suggestions that the government improve technical knowledge among policymakers and judges. Here 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, ensuring no cyber warfare, even social issues in the internet space would be regarded as security related issues.” 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.”
National sovereignty: 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. Chinmayi Arun, Research Director of the Center for Communications Governance at National Law University, told us: “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 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.”

Power of external forces: Other interviewees 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, but Indian companies rarely enjoy that kind of proximity to power. As one interviewee stated: “Even organizations that are supposed to represent corporate interests, whether it is FICCI or NASSCOM, 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 one interviewee told us: “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.”

User rights: Interviewees also prioritized users’ rights. As Rishab Bailey told us: “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 is an excellent example for our government in terms of having a rights based framework domestically, and I think we need one internationally as well.” Arun claimed that: “The main problem I see with the existent work on cyber security 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.”

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, “our 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,” as 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 Salman Waris noted last year in an article, 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. With the advent of internet banking, the Reserve Bank of India has recommended public key infrastructure as the most-favored technology for secure internet banking services, as per its June 2001 guidelines on internet banking.

Interactions and Influence in Policymaking

In their efforts to shape policy outcomes, different stakeholders try to influence public opinion, through print and digital media, and with 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 only 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 local push-back against policies that have human rights impacts is negligible. Most resistance comes from international corporations with something to lose under a different policy framework. As Arun argued: “The international big content platforms, the Googles, the Facebooks, the Yahoos, they 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.”

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. Anja Kovacs argues that in addition to the traditional state monopoly on power, states also now have a monopoly on surveillance, which has important human rights ramifications. Kovacs notes: “If you look at traditional theory about democracy, the idea has always been that you give the state monopoly over the power of violence, and that to balance that monopoly, the citizens get protection of human rights. In a way that the internet and technology now works, you can argue that surveillance has become a new kind of monopoly power that states use. Then if you want to balance the power of the state and the power of the people, protection of human rights in general and the protection of freedom of expression in particular becomes even more important.”

From Civil Society to the Wider Multi-Stakeholder Process

Our first stage research emphasized the role civil society in internet policy. Our preliminary analysis reveals perceptions and facts from this civil society perspective that inform internet policy-making in India. This includes a focus on user rights, differences in the meaning and understanding of security between civil society and government, and a common interest in national sovereignty. Additionally more unexpected perceptions and facts surfaced, including the technology knowledge-deficit in the judiciary and the influence of foreign giants such as Google and Facebook on the government. Our civil society interviewees also expressed that, when it comes to shaping internet policy outcomes, the Indian government has increasingly used national security considerations to shape the debate and maintain its leading role the policy-making process.

Our interviews with civil society organizations involved in India’s internet governance are part of our efforts to learn about (a) the changing power relations that exist in the global multi-stakeholder model, and (b) the ways in which discussions at the national and global levels influence each other and shape policy outcomes. In our interviews with stakeholders, we have sought to understand the interactions and power dynamics at work in India’s internet governance. It is clear that internet policy-making in India is a complex process involving a mix of stakeholders and discussions at the local, national, and global levels. While global discussions of internet governance have been years in the making, national differences (in laws, practices, user culture, and vulnerabilities) continue to persist. In this sense, there is an important and under-studied national element in the governance of global communication networks.
References


6 The Federation of Indian Chambers of Commerce and Industry is an association of business organizations in India.

7 The National Association of Software and Services Companies is a trade association in India’s IT sector.

Featured Photo Credit: CC BY-SA 3.0