Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2016 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-10-2016

Historical Consciousness of Cybersecurity in India

Ramesh Subramanian
Quinnipiac University, ramesh.subramanian@quinnipiac.edu

Historical Consciousness of Cybersecurity in India

Ramesh Subramanian
Quinnipiac University, Hamden, USA {ramesh.subramanian@quinnipiac.edu}

ABSTRACT

This paper examines conceptual developments in the history and evolution of cybersecurity in India. We look at cybersecurity very broadly, starting from the history and development of ICTs, specifically telecommunications in India during the colonial period, their role as a security apparatus to the British, and the continuation and refinement of this role by the Indian government after independence. We trace the evolution of telecommunications and computing in India starting from the 1960s, the expansion of telecommunications infrastructure, the role of ICTs in national security and development, and the gradual ascent of cybersecurity as a security apparatus, and ICT policy deliberations.

Keywords: Cybersecurity history, India, Colonial control, Telecom laws, Culture of security

INTRODUCTION

India's post-liberalization economy has allowed private ICT corporations to emerge and thrive, but the telecommunications sector is still strictly regulated. The agility of private enterprises deeply contrasts with the slower governmental processes with respect to security, privacy and public policy. Interactions affecting the latter are much slower, requiring more deliberations and feedback-response, and access to expertise. Over the last ten years, several well publicized cases have illustrated India's weaknesses in cybersecurity preparedness. In 2011, the Citizen's Lab at the University of Toronto discovered massive infiltration of India government and military computers by foreign attackers (Dharmakumar & Prasad 2011).

We examine the complex set of influences – which include the introduction of telecommunications in colonial India, state control, state and regulatory bodies, history of

legislative actions, think tanks dealing with national cybersecurity, Internet service providers, and content providers, as well as cultural imperatives – through an historical lens with a view to gaining a deeper understanding about the way cybersecurity has evolved in India over time. The methodology we adopt is historiographic research.

COLONIAL INDIA: THE TELEGRAPH, COMMUNICATIONS AND SECURITY

In 1848, James Andrew Broun Ramsay, Marquee of Dalhousie (1812 – 1860), also known as Lord Dalhousie, was appointed the Governor-General of India by the East India Company. His mission was to unify India, a huge landmass comprised of numerous kingdoms, and eventually control it. A new invention known as the telegraph helped him accomplish this objective. The telegraph was patented, almost at the same time, in 1837 by William Cooke and Charles Wheatstone in England, and by Samuel Morse in the US respectively. Independent of these, a British surgeon named William O'Shaughnessy working for the East India Company in India developed his own telegraph system, and set up a 13.5-mile demonstration telegraph system near Calcutta in 1839. When Lord Dalhousie became governor, he authorized O'Shaughnessy to build a 27-mile telegraph line near Calcutta, which was then the headquarters of the British government in India. The first trans-India telegraph lines were laid in 1851 by the British government. The British rulers used the telegraph as an instrument to maintain security and control. In fact, the telegraph was used to transmit strategic communications during the 1857 "Sepoy rebellion," when Indian soldiers mutinied against the British. The strategic use of the telegraph was not lost on the Indians. Lienhard notes that one captured Sepoy rebel, while being led to the gallows, pointed to a telegraph line and cried, "There is the accursed string that strangles us" (Lienhard 1998). H.C. Fanshawe, in his book "Delhi Past and Present" refers to the incident when, during the rebellion, a telegraph signaler at Delhi was cut down with his had still upon the telegraph instrument (presumably signaling information to the British) (Fanshawe 1902, pp108). Aditi Vatsa notes that Sir Robert Montgomery, a British administrator during the

colonial times, had remarked after the mutiny that "the electric telegraph had saved India"(Vatsa 2012).

In 1854, the first Telegraph Act was passed under Lord Dalhousie, and unlike England, the telegraph was made into a government monopoly. This, and the subsequent Act in 1860 granted the government powers to take possession of leased telegraph lines (and thus gain possession of the telegraphs that were transmitted) upon any public emergency (Acharya 2015). Daniel Headrick notes that Lord Dalhousie viewed the telegraph not as a business enterprise, but as an instrument of British power in India (Headrick 1991).

After the rebellion, the telegraph spread rapidly in India, primarily for military purposes. It was also eventually opened up to commercial enterprises and the public, though control was strictly maintained by the government. As the use of the telegraph for commercial purposes grew, so began its deliberate misuse – i.e., selling of crucial commercial information in the open market by under-paid government telegraph operators. Halford Hoskins noted that there was "malicious misconstruction of messages whenever native merchants may profit from these errors, and it was an open scandal that commercial intelligence was peddled in Indian markets by Government telegraph clerks" (Hoskins 1928, pp. 386). These can be considered to be examples of early 'telecommunications breaches' in India.

More versions of the Telegraph Act followed. The Telegraph Act of 1876 reinforced the government's power to possess leased telegraph lines during public emergencies *as well* as in cases deemed to be of public interest. This Act was superseded by the Telegraph Act of 1885, which granted the government the power to order interception of messages during public emergencies as well as for public interest.

Telecom Developments in Late 19th and early 20th Century

In 1881 the government granted permission to the Oriental Telephone Company to set up exchanges in five cities (BSNL Calcutta Telecom District 2012). By 1884 the telephone was

combined with the telegram service, and telegrams were beginning to be sent and received by telephones (Mann 2015). Telephones came completely within the purview of the Telegraph Act of 1885. In that Act, the definition of "Telegraph" included "telephonic or other communications by means of electricity, galvanism or magnetism" (The Governor General of India 1885). By the early 1920s wireless telegraphy was replacing wired telegraphy. To address this technology development, the Indian Wireless Telegraphy Act was enacted in 1933. This Act treated wireless telecommunications as a simple appendix to the telegraph, and thus nothing substantially different was added to the Telegraph Act of 1885.

These early examples show how communication control, strict governmental oversight of telecommunications, as well as surveillance through wiretapping were well established in India during colonial times through a series of telegraph statutes. These statutes, which show the colonizer's interest in maintaining control and power over the colonized, survived unchanged for 87 years, well after India gained independence from the British in 1947.

INDEPENDENCE: CONTINUING THE BRITISH TELECOM SECURITY LEGACY

After India gained independence in 1947, the Indian government was determined to attain security and self-sufficiency without the help or assistance of any other nation. Indigenous industrial development was the "mantra" of the newly formed nation and its leaders. The Indian government decided that telephone and telegraph systems would be a government monopoly administered by its own civil service (Menon 1999). Thus, at the time of independence, all foreign telecommunications companies were nationalized to create the Posts and Telegraphs Department (P & T), a state-run monopoly. In doing this, the central government retained complete control of telecommunications, a legacy of British colonial rule.

Free Speech, Privacy and the Constitution

The Indian Constitution (1949) guarantees the right to free speech, but also stipulates that this right can be deprived under nine extenuating conditions. These are listed in Article 19(2). But the

Telegraph Act of 1885 left the terms "public emergencies" and "public interest" deliberately vague, and to the discretion of the government. This "gap" was however plugged by the 1972 amendment to the Telegraph Act under Indira Gandhi's rule (discussed in the next section). The Indian Constitution also does not explicitly guarantee privacy. Article 21 states that "no person in the country may be deprived of his life or personal liberty except according to procedure established by law" (Human Rights Watch 1999). It does not explicitly state anything about an individual's right to privacy. The first connection between Article 21's granting of "personal liberty" and an individual's privacy rights in India was established in the 1964 Supreme Court ruling in the *Kharak Singh v. State of Uttar Pradesh* case (Agarwala 1996, para 4). Kharak Singh had complained in his lawsuit that his right to privacy was being violated by the police of the State, who made domiciliary visits to his place of residence and harassed him. The Court repelled his argument, but the minority judgment emphasized the need to recognize the right to privacy "as it was an essential ingredient of personal liberty." From that time on, the right to privacy has gradually become accepted as a right granted through Article 21 of the Constitution, and has been applied to various situations.

Thus Article 19 guarantees free speech, and Article 21 has generally come to be accepted as recognition of individual's right to privacy. However, the combination of these two articles fail to address the issue of wiretapping that is allowable under the Telegraph Act of 1885, which was adopted by India after independence.

Phone Tapping in India

Wiretapping (or phone tapping) private citizens' telephones has routinely been employed by Indian security agencies at the behest of the government in power, mostly to harass opposition politicians. The wording of the Telegraph Act was ambiguous enough that the government has often used this as a weapon, usually claiming that there existed a threat to society at large. Since

telecommunications was until recently completely controlled and run by the government, this was easily achievable in practice.

Phone tapping of members of opposition parties became widespread in the 1970s and 1980s (The Lewiston Daily 1981, page 32). In 1971 Prime Minister Indira Gandhi, citing internal and external security threats, oversaw the enactment of the Defense and Internal Security of India Act 1971 (DISA), which gave the government fresh powers to wiretap. These powers were not subject to even the minimal protections of the Telegraph Act. In 1972, the Indian Telegraph Act 1885 was amended by HN Bahuguna, the Communications Minister, to include five "conditions" from Article 19(2) of the Constitution that provide more explicit situations under which a threat to public interest or an internal emergency could be perceived. This amendment further reduced privacy protection by actually enhancing the powers of the government to intercept messages even if there was a threat of "incitement of offences" (Dhavan 2000). This amendment provided more ammunition to the party in power at the moment. During the years 1975 to 1977, Mrs. Indira Gandhi, fearing electoral disqualification, declared a "state of Emergency" and took total power over India. India became a near-totalitarian state, and numerous civil and human rights violations were committed. The ordinarily free press was severely censured, and the telephone conversations of opposition politicians, members of the press and even university professors were secretly intercepted, thus abusing the provisions of the Indian Telegraph Act. These incidents have been widely reported in the press. However, no single political party in India can be solely implicated in the numerous wiretapping scandals that have been exposed periodically. Over the years, every party in power has resorted to this practice against opposition politicians. The list of those whose phones have been tapped include the former Prime Minister, Mr. Chandra Shekar (in 1991), who had been subjected to wiretapping before he assumed office by his political opposition, the National Front, headed by V.P. Singh; and the former President of India, Zail Singh, by the government led by Rajiv Gandhi (between

the period from 1984 to 1987) (The Hindu (Opinion) 2006). The free press played an important role in exposing the phone tapping scandals in India during this period in India's history.

Wireless Telecommunications

As wireless telecommunications gained ground in India in 1995, new problems surfaced. New geopolitical developments and increased terrorist activities required the government to have interceptive powers to extend to mobile telecommunications also. This was easily achievable, as the government's Department of Telecommunications was the sole licensing authority for private operators offering wireless services. It simply added a clause through which operators would be obliged to provide dedicated surveillance lines to identified government agencies, such as the Intelligence Bureau (IB) and the Central Bureau of Investigation (CBI) (The Indian Express 2006).

INTERNET AND THE INFORMATION TECHNOLOGY ACT OF 2000

By the early 1980s, it became apparent to the politicians, industrialists and large sections of the intelligentsia that the socialist policies had not succeeded. In 1984, facing a severe foreign-exchange reserve problem, the Indian government finally ushered in some liberalized economic policies under the Prime Minister-ship of Rajiv Gandhi. In 1991, Manmohan Singh, India's Finance Minister under the PV Narasimha Rao, further liberalized the economic policies. A new industrial policy (NIP) vastly easing onerous industrial license policies and import restrictions on high technology was announced. Export-oriented ventures were given tax incentives. Foreign direct investments (FDIs) were welcomed in all sectors.

In 1986 the government's Department of Electronics (DOE) obtained a funding of $6 million from the UNDP to create the Education and Research in Computer Networks (ERNET). ERNET was formally connected to the Internet on February 12, 1989 (Ramakrishnan 2009). Initially, ERNET was limited to researchers and employees at seven elite academic and research institutions and the government's Department of Telecommunications (DOT), and ERNET staff.

The DOT permitted public access to the Internet in 1995, and the government-run VSNL was the first public-access ISP in India. Later, in 1998, the DoT announced the private ISP policy.

Realizing the vast potential of information technology, the Indian government began to take some critical steps towards fostering and engendering growth in this sector. In 1998, Prime Minister Atal Behari Vajpayee set up a "National Task Force on IT and Software Development." The resulting ideas and suggestions were collected and developed into an "Information Technology Action Plan," which consisted of 107 "objectives," categorized under several areas such as "Info-Infrastructure Drive," export targets for IT software and services, strategies for creating IT penetrations and awareness, Citizen IT interfaces, IT in Government, and development of Data Security Systems and Cyber Laws (IT-Taskforce-NIC 1998). Objectives 100 to 107 pertained to "Data Security Systems and Cyber Laws," and envisaged the creation of an Information Security Agency, cybersecurity laws, national cybersecurity policy, digitizing data and record-keeping. The IT Plan was used to create the Information Technology Act of 2000.

CYBERSECURITY CONSCIOUSNESS

The IT Act of 2000 aims "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies…" (Ministry of Law, Justice and Company Affairs 2000). The Act addresses many issues pertaining to the conduct of e-commerce, such as digital signatures, public key infrastructure, e-governance, cyber contraventions, cyber offences and confidentiality and privacy. Thus, some of the issues of security and interception under the telegraph and telephone regimes were now extended to the realm of the Internet, and thus were subsumed under the notion of "cybersecurity."

Today more and more middle-class Indians use the Internet for information, shopping and banking. Viruses, malware, phishing and identity-theft incidents have slowly but surely caused increased awareness of the importance of securing personal information. Cybersecurity is becoming important not just for the state, but also for its citizens. Indian citizens are becoming collectively conscious of privacy on the Internet, security of personal data, and along with that, surveillance by the government.

There is also the realization that just as in the case of telegraphs and telephones, the government was not eager to keep the Internet completely open and free of any type of censorship or surveillance. In subsequent years the IT Act has faced criticism for being too expansive and for undermining privacy and free speech (Holder & Grimes 2006). An example of its expansiveness is seen in 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 provides to data is with respect to the penalty in cases of breach or unlawful activity (Bharadwaj 2010).

Three years after passage of the IT Act, the Indian government formalized its process for blocking websites. Through "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 2003).

However, growing opposition to the government's approach to cybersecurity was effectively nullified by the after the 2008 Mumbai terrorist attacks. In the weeks following, 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 2013). 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 such 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.

Article 66A of the IT Amendment Act

The above statement notwithstanding, there are signs of change. Working in coordination with the free press, the civil society actors are beginning to make concerted action 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.

CYBERSECURITY – 2014 AND BEYOND

The Indian government has progressively introduced restrictions on the Internet. However, despite its thriving IT industry and its IT acumen, it has proven to be less than adept when responding to the global threat of cyber-attacks. With the proliferation of mobile telephony and Internet access through smartphones, India has become a prime target for cyber criminals and cyber-attacks. As noted in the Introduction section, the Citizen's Lab at the University of Toronto reported massive infiltration of India's government and military computers in 2011 (Dharmakumar & Prasad 2011). A 2014 report by the Kaspersky Lab placed India second on a list of most cyber-attacks on mobile devices (Press Trust of India 2014). The 2015 Symantec "Internet Security Threat Report" listed India as one of the top five countries to be affected by cybercrime, and second in terms of malicious software originating from a particular country (Symantec 2015). Despite these escalating cyber-attacks, qualified cybersecurity professionals in India in 2013 was less than a thousand!

Realizing the problem, the Indian Government's Ministry of Information Technology released a "National Cybersecurity Policy (NCP)" in 2013. Some of the key objectives listed in

this policy statement were: Strengthen regulatory framework; create assurance framework; create indigenous security technologies; protect national information infrastructure; create standards; develop 500,000-person cybersecurity workforce by 2017. However, in early 2015 the "52nd Standing Committee on IT conducted a review on the implementation of the NCP. The results were not encouraging. According to the committee's report, the cybersecurity policy directions set forth in the NCP are yet to be implemented. Work on a comprehensive Privacy Bill has stopped. Many structural issues still remain. For instance, the Indian government budgeted just $7.76 million for cyber security in 2013, compared with at least $751 million spent by the U.S. government on its cyberspace programs. There is still a great lack of qualified cybersecurity professionals in India.

ANALYSIS AND CONCLUSIONS

Cybersecurity of nations is a critical issue at present. It affects the economy as well as the basic functioning of a society. There are numerous threats to cybersecurity, both internal and external. The way in which a nation attempts to address cybersecurity is often rooted in its history – historical ways in which the state has used its communications infrastructure to control and maintain power vis-à-vis use it as a developmental tool. India, with is history of colonization falls primarily in the former category, in which the information and communications infrastructure was used by the British rulers as a tool to control. During the colonial rule various laws were enacted that allowed the government to curb the free flow of information, as well as to surveil, and intercept messages of citizens. There were serious violations of privacy, mostly because it was generally assumed that colonized citizens were not eligible to enjoy the same rights as the colonizers.

It would be reasonable to assume that these laws would have changed after India gained independence, considering that India chose to follow a democratic political structure. However, as seen above, the Indian rulers were content to maintain status quo when it came to control and

interception of messages of the citizens. The initial motive seems to have been an aversion to foreign ideas, and ergo, the compulsion to control such ideas and not let new ideas take root among Indian citizens. Later, such control mechanisms became useful tools for the ruling parties to maintain power and restrict the voices of the opposition parties.

Over time, the voices of democracy and civil society has begun to prevail, and formerly restrictive laws have been amended to incorporate more transparent procedures. But in most cases, such transparency has had to be fought for in the Courts. The role of the press and civil society have been indispensable in this.

At present, the main threat to the nation's security comes in the form cyber threats. Thus cybersecurity has emerged as the most important policy issue that affects the security of India. The government seems to have taken some baby steps towards achieving cyber security. However, as noted above, this is a work very much in progress. There is always the threat of governmental over-reach, wherein the need to preserve national security is compared with the citizens' need for privacy. It is important for both policy makers as well as citizens to seek and achieve the right balance, i.e. implement cybersecurity with a focus on balancing national security with privacy concerns.

REFERENCES

Acharya, B. 2015, May 30). Mastering the Art of Keeping Indians Under Surveillance. Retrieved from http://thewire.in/2015/05/30/mastering-the-art-of-keeping-indians-under-surveillance-2756/

Agarwala, B. D. 1996). Right to Privacy: A Case-By-Case Development. *Supreme Court Cases*, *3*(9). Retrieved from http://www.ebc-india.com/lawyer/articles/96v3a2.htm

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

BSNL Calcutta Telecom District. 2012. History and Growth of Calcutta Telephones. Retrieved June 3, 2016, from http://www.calcutta.bsnl.co.in/mainfooter/MainFooter_Company.html

Dharmakumar, R., & Prasad, S. 2011, September 19. Hackers' Haven. Retrieved May 14, 2015, from http://forbesindia.com/printcontent/28462

Dhavan, R. 2000, April 21. The Hindu : Tapping Mr. Cronje. Retrieved June 4, 2016, from http://www.thehindu.com/2000/04/21/stories/05212523.htm

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

Fanshawe, H. C. 1902. *Delhi Past and Present*. London: John Murray, Albemarle Street.
Headrick, D. R. 1991. *The Invisible Weapon: Telecommunications and International Politics, 1851-1945*. New York, NY, USA: Oxford University Press.
Holder, J. T., & Grimes, D. E. 2006. Government Regulated Data Privacy: The Challenge for Global Outsourcers. *Georgetown Journal of International Law*, *38*, 695–712.
Hoskins, H. L. 1928. *British Routes to India*. Universitiy of Pennsylvania.
Human Rights Watch. 1999. Selected Articles of the Indian Constitution - Broken People: Caste Violence Against India's "Untouchables" (Human Rights Watch Report, 1999). Retrieved June 4, 2016, from https://www.hrw.org/reports/1999/india/India994-15.htm
IT-Taskforce-NIC. 1998. IT Taskforce : Information Technology Action Plan. Retrieved June 4, 2016, from http://it-taskforce.nic.in/it2008.htm
Lienhard, J. H. 1998. No. 1380: Indian Telegraph. *Engines of our ingenuity*. Houston, TX: Houston Public Media. Retrieved from http://www.uh.edu/engines/epi1380.htm
Mann, M. 2015, August 2. Telecommunication and the Public Sphere in British India, 1850-1950 — Institute of Asian and African Studies [Page]. Retrieved June 3, 2016, from https://www.iaaw.hu-berlin.de/en/region/southasia/research/projects/completed/communication
Menon, A. R. 1999, May. *India: Adopting a Pro-Competitive Policy for Telecommunications*. Retrieved from http://www.commercialdiplomacy.org/ma_projects/ma_india1.htm#the%20history%20of%20telecommunications%20services%20in%20india
Ministry of Communications and Information Technology. 2003, February 27. Notification no. G.S.R.181(E). Retrieved June 4, 2016, from http://www.naavi.org/cl_editorial_06/notification_270203_blocking.htm
Ministry of Law, Justice and Company Affairs. 2000, June 9. The Information technology Act, 2000 | The Gazette of India. Retrieved June 4, 2016, from http://cca.gov.in/cca/sites/default/files/files/act2000_0.pdf
Moody, G. 2011, November 2. India Wants UN Body To Run The Internet: Would That Be Such A Bad Thing? | Techdirt. Retrieved June 4, 2016, from https://www.techdirt.com/articles/20111102/04561716601/india-wants-un-body-to-run-internet-would-that-be-such-bad-thing.shtml
NASSCOM. 2015. India IT-BPM Overview | NASSCOM. Retrieved September 8, 2015, from http://www.nasscom.in/indian-itbpo-industry
Nehru, J. 1946. *The Discovery of India*. Calcutta: The Signet Press.
Prakash, P. 2013, July 10. How Surveillance Works in India - The New York Times. Retrieved June 2, 2016, from http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=1
Press Trust of India. 2014, March 2. India second on cyber attacks on mobile | The Indian Express. Retrieved May 14, 2015, from http://indianexpress.com/article/india-others/india-second-on-cyber-attacks-on-mobile/
Ramakrishnan, S. 2009, August 23. Interview with Kishore Bhargava.
Sriram, J. 2015, March 25. SC strikes down "draconian" Section 66A - The Hindu. Retrieved May 1, 2015, from http://www.thehindu.com/news/national/supreme-court-strikes-down-section-66-a-of-the-it-act-finds-it-unconstitutional/article7027375.ece
Subramanian, R. 2011. The Growth of Global Internet Censorship and Circumvention – A Survey. *Communications of the Association for Information Systems*, *11*(2). Retrieved from 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

Symantec. 2015, April 15. 2015 Internet Security Threat Report, Volume 20 - 21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf. Retrieved May 15, 2015, from https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf

The Governor General of India. The Indian Telegraph Act, 1885 (1885).

The Hindu (Opinion. 2006, January 6. Phone tapping issues. *The Hindu*. Retrieved from http://www.thehindu.com/todays-paper/tp-opinion/article3235846.ece

The Indian Express. 2006, January 4. Tips for a tap. Retrieved June 4, 2016, from http://archive.indianexpress.com/oldStory/85224/

The Lewiston Daily. 1981, July 30. Phone Tapping Alleged. Retrieved June 4, 2016, from https://news.google.com/newspapers?nid=1928&dat=19810730&id=1fYpAAAAIBAJ&sjid=f2cFAAAAIBAJ&pg=2168,5629368&hl=en

Vatsa, A. 2012, November 18. When telegraph saved the empire - Indian Express. Retrieved June 19, 2016, from http://archive.indianexpress.com/news/when-telegraph-saved-the-empire/1032618/