IP ADDRESSES AND EXPEDITIOUS DISCLOSURE OF IDENTITY IN INDIA

*Prashant Iyengar**

Concomitant with the proliferation of cybercrime in India has been the use of Internet Protocol (IP) addresses by law enforcement agencies to track down criminals. While useful in many situations, the potential for misuse of this information raises important concerns for the privacy of individuals online. This note reviews the statutory mechanisms regulating the retention and disclosure of IP addresses by internet companies in India. It identifies and analyses the four broad sources to which the regime of IP Address disclosure by Internet Service Providers (ISP) may be traced: under the (i) operating licenses issued under the Telegrah Act, 1885, (ii) Information Technology Act, 2000, (iii) Code of Criminal Procedure, 1973 (hereinafter, "the Cr.P.C.") and (iv) contractual agreements between users and ISPs. It concludes that the various layers of Indian law create an atmosphere that is intensely hostile to the withholding of such information by ISPs and intermediaries. Despite this, the author submits that there remains scope for optimism.

Introduction

With the rise in the number of users in the past decade, the internet has become an extremely fraught space that has been frequently used for the perpetration of a range of cyber crimes, including extortion, defamation and financial fraud. In a revealing statistic, in 2010, the Mumbai Police reportedly "received 771 complaints about internet-related offences, *319 of which were from women who were the victims of fake profiles, online upload of private photographs and obscene emails*."[1] This high incidence of women victims indicates that the relatively anonymous 'open' architecture of the internet has yielded disempoweringly discriminatory consequences for women, who tend to be easy targets of humiliation, harassment or blackmail online.

* Prashant Iyengar is Assistant Professor & Assistant Director, Centre for Intellectual Property Rights Studies. He has an (LL.M.) with honors from Columbia Law School and a B.A.B.L. (Hons.) from NALSAR, University of Law, Hyderabad. Earlier, he was Lead Researcher with Privacy India, Bangalore; Legal Aid Manager with Rural Development Institute, Hyderabad; Researcher & Lawyer with Alternative Law Forum, Bangalore and was Guest faculty with Christ Law College, Bangalore.

[1] Mateen Hafeez, *A tangled web of vengeance*, TIMES OF INDIA (Mar. 28, 2011, 5:44 AM), http://articles.timesofindia.indiatimes.com/2011-03-28/mumbai/29353669_1_boyfriend-social-networking-police-officer.

Law enforcement authorities in India have not exactly lagged behind in bringing these new age cyber criminals to book, and have set up special 'Cyber Crime Cells' in different cities to combat crimes on the internet. These cells have been particularly adept at using IP addresses' information to trace the individuals responsible for these crimes. Very briefly, an Internet Protocol address (hereinafter, "IP address") is a numeric label – a set of four numbers (e.g., 202.54.30.1) – that is assigned to every device (e.g., computer, printer, mobile phone) participating on the internet.[2] Website operators (such as Google) and Internet Service Providers ("ISPs", such as Airtel or BSNL) typically maintain data logs that track the online activity of every IP address that accesses their services. Although IP addresses refer to particular computers – not necessarily individual users – it is possible, through further investigation, to trace these addresses backwards to expose the individual behind the computer.[3] As even a casual Google search with the phrase "IP, police, India" would reveal, police authorities in different cities in India have successfully and quite happily employed this new technology to trace culprits.

However, along with its utility in the detection of crime, the tracking of persons by their IP addresses is potentially invasive of individuals' privacy – itself a weak, embattled legal right in India. In the absence of a culture of strict adherence to the 'rule of law' by the police apparatus in India, the unbridled ability to track persons through IP addresses has the potential of becoming an extremely oppressive tool of pervasive surveillance.

In addition, several alarming incidents in the past year have made it clear that the Indian Government has found in this technology a reliable ally with which it may stamp out political dissent, or even satire and unfavourable comment, on the internet. These incidents raise questions of free speech and censorship, which are superadded to the concerns of privacy.

In this short note, I review the statutory mechanism regulating the retention and disclosure of IP addresses by internet companies in India. Increasingly in Indian scholarship and in the courts, it has become uncommon to attempt to tie executive action to any specific legislative mandate. In order to

---

[2] *IP address*, WIKIPEDIA, http://en.wikipedia.org/wiki/IP_Address (last visited June 15, 2011).

[3] McIntyre, Joshua J., Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected as Personally Identifiable Information (August 15, 2010). DePaul Law Review, Vol. 60, No. 3, 2011. Available at SSRN: http://ssrn.com/abstract=1621102 [Accessed June 21, 2012]

provide context, I begin with a compilation of anecdotes on how various law enforcement authorities in India have used IP address information to trace individuals responsible for particular crimes.

Examples of Use and Abuse by Indian Authorities

As mentioned above, over the past several years, internet media has been humming with stories which indicate the extent to which IP addresses have become a useful and frequently deployed weapon in the arsenal of law enforcement agencies and courts:

a) In May 2010, an Army officer stationed in Mumbai was arrested for distributing child pornography from his computer.[4] He was traced by the Mumbai Police after the German Federal Police alerted Interpol that objectionable pictures were being uploaded from the IP address he was using.

b) In February 2011, Cyber Crime Police in Mumbai sought the IP address details of a user who had posted 'Anti Ambedkarite' content on Facebook, the popular social networking website.[5]

c) In February 2008, the internet search company Google was ordered by the Bombay High Court to reveal "particulars, names and the address of the person" who had posted defamatory content against a company on Google's blogging service, Blogger.[6]

---

[4] *Army officer held in city for child porn*, TIMES OF INDIA (May 8, 2010, 1:59 AM), http://articles.timesofindia.indiatimes.com/2010-05-08/mumbai/28292650_1_hard-disks-obscene-clippings-downloading.

[5] *Anti-Ambedkar page on Facebook blocked*, HINDUSTAN TIMES (Feb. 17, 2011, 2:45 AM), http://www.hindustantimes.com/Anti-Ambedkar-page-on-Facebook-blocked/Article1-663383.aspx.

[6] David Sarokin, *Google Ordered to Reveal Blogger Identity in Defamation Suit in India: Gremach Infrastructure vs Google India*, SAROKI6965 BLOG (Aug. 15, 2008), http://saroki6965.wordpress.com/article/google-ordered-to-reveal-blogger-l9cm7v116zcn-7/.

d) In September 2009, a man was arrested by the Delhi Police in Mumbai for blackmailing classical musician Anoushka Shankar. The culprit had allegedly hacked into her e-mail account and downloaded copies of personal photographs. He was traced by using his IP address.[7]

e) In April 2010, the Gurgaon Police arrested a teenage boy for allegedly posting obscene messages about an actress on Facebook. The newspaper account reports that:

> During investigations, the police browsed through several service providers and finally zeroed in on BSNL, which helped them trace the sender's IP address to someone called 'Manoj Gupta' in Gurgaon. A team of policemen were sent to Gurgaon but the personnel found out that Manoj Gupta was [a] fictitious name which the teenager was using in his IP address. The police arrested the accused as well as seized the hardisk [sic] of his personal computer.[8]

f) In February 2011, the police traced a missing boy who had run away from home, by following the IP address trail he left when he updated his Facebook profile status.[9]

g) In March 2013, the Mumbai Police tracked down a girl who had sent an e-mail to a newspaper threatening to commit suicide on account of her poor 12th standard examination results.[10]

What is clearly evident from these accounts is a growing awareness and enthusiasm on the part of Indian law enforcement agencies to use IP address trails as a routine part of their criminal investigation process. While this is not unwelcome, considering the kinds of grievances listed above and the backdrop of a dismal record of criminal enforcement in India, there is also a flip side to consider. In

---

[7] *Delhi police arrest man for blackmailing Anoushka Shankar*, REDIFF (Sept. 20, 2009, 4:51 PM), http://news.rediff.com/report/2009/sep/20/police-arrest-man-for-blackmailing-anoushka-shankar.htm.

[8] S. Ahmed Ali, *Cyber cell nets Delhi teen for lewd online posts*, TIMES OF INDIA (Apr. 29, 2010, 6:11 AM), http://articles.timesofindia.indiatimes.com/2010-04-29/mumbai/28116011_1_cyber-cell-cyber-police-abusive-messages.

[9] Mateen Hafeez, *Police find runaway student "online"*, TIMES OF INDIA (Feb. 17, 2011, 1:42 AM), http://articles.timesofindia.indiatimes.com/2011-02-17/mumbai/28554314_1_social-networking-networking-site-sim-card.

[10] *Cop pep talk a balm for suicidal Class 12 girl*, DNA INDIA (Mar. 8, 2013, 6:45 AM), http://www.dnaindia.com/mumbai/1808695/report-cop-pep-talk-a-balm-for-suicidal-class-12-girl.

a shocking incident in August 2007, Lakshmana Kailash, a software engineer from Bangalore, was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the social-networking site Orkut.[11] The police identified him based on IP address details obtained from Google and Airtel, Lakshmana's ISP. He was brought to Pune and jailed for fifty days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not clearly specified whether the suspect had posted the content at 1:15 p.m. or a.m.

Taking cognisance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered Airtel to pay Rs 2 lakh to Lakshmana as damages.[12] This incident sounds a cautionary note, amidst so many celebratory accounts, signalling that grave human rights abuses could result from the unbridled use of this technology.

In an eerily similar incident, in April 2011, a 65 year old man was arrested in Pune and later prosecuted for allegedly posting obscene photographs of a woman on Facebook. During the trial, it was realised that the police had arrested the wrong person since "the social media firm sent dates in the normal US format of 'month-day-year' (MM/DD/YY). But the police read it in the Indian format of 'day-month-year' (DD/MM/YY)." The newspaper account goes on to report that he has filed a Public Interest Litigation before the Supreme Court, seeking the framing of appropriate guidelines to ensure such errors do not recur. [13]

These are just a few out of scores of instances of Indian investigative authorities tracing culprits using IP addresses. The offences alleged range from blackmail to impersonation, and from defamation to planning terror attacks. Seldom in these cases has a court order actually been required by the agency that discloses the IP address of the individual.[14] Clearly, there seems to be a very easy relation between

---

[11] Anand Holla, *Wronged, techie gets justice 2 yrs after being jailed*, MUMBAI MIRROR (June 25, 2009, 3:14 AM), http://www.mumbaimirror.com/mumbai/others/Wronged-techie-gets-justice-2-yrs-after-being-jailed/articleshow/15934351.cms.

[12] *Id.*

[13] Utkarsh Anand, *Cops mix up dates, 65-yr-old in cyber soup*, INDIAN EXPRESS (Mar. 2, 2013, 2:39 AM), http://www.indianexpress.com/news/cops-mix-up-dates-65yrold-in-cyber-soup/1082000/0.

[14] This is not atypical. In the US, for instance, as Joshua McIntyre writes:

law enforcement agencies in India on the one hand, and Internet Service Providers and online services such as Google and Facebook on the other.

Google's own 'Transparency Report'[15] which provides statistics on the number of instances where Government agencies have approached the company demanding information or take-down, states that it received close to 4700 'data requests' from Indian authorities between January to December 2012 – ranking India 2nd globally in terms of such requests, behind the United States. That a high percentage – 64-66% – of these requests have reportedly been complied with indicates that within a short span of time, Indian authorities have discovered in Google a reliable and pliable ally in seeking information about their subjects. In 2007, Orkut, a social-networking website owned by Google, even entered into a co-operation agreement with the Mumbai Police in terms of which "'forums' and 'communities'" which contained "defamatory or inflammatory content" would be blocked, and the IP addresses from which such content had been generated would be disclosed to the police.[16]

> While various federal statutes protect similar data such as telephone numbers and mailing addresses as Personally Identifiable Information (PII), federal privacy law does not generally regard IP addresses as information worthy of protection. It has, therefore, become commonplace for litigants to subpoena ISPs to unmask online speakers. *Many ISPs have no reason to fight these subpoenas and readily give up their subscribers' names, addresses, telephone numbers, and other identifying data without demanding any court oversight or providing any notice to the subscriber. Even when courts become involved, a full consideration of the online speaker's privacy interests is far from certain*. (emphasis added)

MCINTYRE, *supra* note 3, at 5.

15 *Google Transparency Report: User Data Requests – India*, GOOGLE.COM, http://www.google.com/transparencyreport/userdatarequests/IN/ (last visited Apr. 4, 2013).

16 *Orkut's tell-all pact with cops*, ECONOMIC TIMES (May 1, 2007, 9:00 AM), http://articles.economictimes.indiatimes.com/2007-05-01/news/28459689_1_orkut-ip-addresses-google-spokesperson.

Although similar transparency reports are not forthcoming from the other Internet giants such as Hotmail,[17] Yahoo[18] or Facebook,[19] there is overwhelming anecdotal evidence that this co-operation has not been withheld by them.

In the sections that follow, I shall outline the legal framework that facilitates this co-operation between law enforcement authorities and web service providers.

Lawful Disclosure of IP Addresses

In this section, we are seeking a legal source for the compulsion of ISPs and intermediaries (including websites) to disclose IP address data. Are there any guidelines in Indian law on how much information must be disclosed, under what circumstances and for how long?

Broadly, there are four sources to which we may trace this regime of disclosure and co-operation. *First*, ISPs are required, under the operating license they are issued under the Telegraph Act, 1885, to provide assistance to law enforcement authorities which, under certain circumstances, include turning over all user records. *Secondly*, the Information Technology Act, 2000 (hereinafter, "the IT Act") contains provisions which empower law enforcement authorities to compel the disclosure of information from those in charge of any 'computer resources'. Reciprocally, 'intermediaries' – including ISPs and websites – are charged under new Rules under the IT Act with co-operating with government agencies on pain of exposure to financial liability. *Thirdly*, the Code of Criminal Procedure, 1973 (hereinafter, "the Cr.P.C.") defines the scope of police powers of investigation, which include powers to interrogate and summon information. *Fourthly*, individual subscribers enter into contracts with ISPs and web services which do not offer any stiff assurances of privacy with regard to IP address details.

---

[17] In June 2011, Hotmail supplied IP address details which enabled the Delhi Police to trace, with further assistance from Airtel, the sender of obscene e-mails to a noted actress. Mohit Sharma, *Priyanka Chopra's cousin harassed in Delhi*, MID-DAY (June 10, 2011), http://www.mid-day.com/news/2011/jun/100611-news-delhi-priyanka-chopra-cousin-Meera-Chopra-harrassed.htm.

[18] Alok K.N. Mishra, *Man who sent hoax email to DGP nabbed*, TIMES OF INDIA (Jan. 1, 2013, 4:50 AM), http://articles.timesofindia.indiatimes.com/2013-01-01/ranchi/36093637_1_hoax-email-cyber-cafe-hoax-mail.

[19] ANAND, *supra* note 14.

The sections that follow offer greater detail on each of these areas of the law.

1. Monitoring of Internet Users under the ISP Licenses

ISPs are regulated and operate under a license issued under the Telegraph Act, 1885. Section 5 of the Telegraph Act empowers the Government to take possession of 'licensed telegraphs' and to order interception of messages in cases of 'public emergency' or 'in the interest of the public safety'. Interception may only be carried out pursuant to a written order by an officer specifically empowered for this purpose by the State or Central Government. The officer must be satisfied that "it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence."20

Although the statute governs the actions of ISPs in general, more detailed guidelines regulating their behaviour are contained in the terms of the licenses issued to them, which set out the conditions under which they are permitted to conduct business. The Internet Services License Agreement, which authorises ISPs to function in India, contains provisions requiring telecom operators to safeguard the privacy of their consumers and to co-operate with government agencies when required to do so. Some of the important clauses in this Agreement are:

a) Part VI of the License Agreement gives the Government the right to inspect or monitor the ISPs' systems. The ISP is responsible for making facilities available for such interception.

b) Clause 32 under Part VI contains provisions mandating the confidentiality of information held by ISPs. These provisions hold ISPs responsible for the protection of privacy of

20 In 1997, in PUCL v. Union of India (AIR 1997 SC 568), the Supreme Court of India held that the interception of communications under this Section was unlawful unless carried out according to the procedure established by law. Since no Rules had been prescribed by the Government specifying the procedure to be followed, the Supreme Court framed guidelines to be followed before tapping of telephonic conversations. These guidelines have been substantially incorporated into the Indian Telegraph Rules in 2007. Rule 419A stipulates the authorities from whom permission must be obtained for tapping, the manner in which such permission is to be granted and the safeguards to be observed while tapping communication. The Rule stipulates that any order permitting tapping of communication would lapse (unless renewed) in two months. In no case would tapping be permissible beyond 180 days. The Rule further requires all records of tapping to be destroyed after a period of two months from the lapse of the period of interception.

communication, and to ensure that unauthorised interception of messages does not take place. Towards this, ISPs are required:

a. to take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and their business to which they provide service and from which they have acquired such information by virtue of that service, and shall use their best endeavours to secure that;

b. to ensure that no person acting on behalf of the ISPs divulges or uses any such information, except as may be necessary in the course of providing such service to the third party.

This safeguard, however, does not apply where:

i. the information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or

ii. the information is already open to the public and otherwise known.

c. to take necessary steps to ensure that any person(s) acting on their behalf observes confidentiality of customer information.

c) Clause 33.4 makes it the responsibility of the ISP to trace nuisance, obnoxious or malicious calls, messages or communications transported through its equipment.

d) Clause 34.8 requires ISPs to maintain a log of all users connected and the service they are using (mail, telnet, http etc.). The ISPs must also log every outward login or telnet through their computers. These logs, as well as copies of all the packets originating from the Customer Premises Equipment (CPE) of the ISP, must be available in real time to Telecom Authority. This clause forbids logins where the identity of the logged-in user is not known.

e) Clauses 34.12 and 34.13 require the ISP to make available a list of all subscribers to its services on a password protected website for easy access by Government authorities.

f) Clause 34.16 requires the ISP to activate services only after verifying the *bona fides* of the subscribers and collecting supporting documentation. There is no Regulation governing how long this information is to be retained.

g) Clause 34.22 makes it mandatory for the Licensee to make available "details of the subscribers using the service" to the Government or its representatives "at any prescribed instant".

h) Clause 34.23 mandates that the ISP maintain "all commercial records with regard to the communications exchanged on the network" for a period of "at least one year for scrutiny by the Licensor for security reasons and may be destroyed thereafter unless directed otherwise by the Licensor".

i) Clause 34.28(viii) forbids the ISP from transferring the following information to any person or place outside India:

   a. Any accounting information relating to subscribers (except for international roaming/billing) (Note: It does not restrict a statutorily required disclosure of a financial nature); and

   b. User information (except that pertaining to foreign subscribers using an Indian Operator's network while roaming).

j) Clause 34.28(ix) and (x) require the ISP to provide traceable identity of its subscribers and on request by the Government, must be able to provide the geographical location of any subscriber at any given time.

k) Clause 34.28(xix) stipulates that "in order to maintain the privacy of voice and data, *monitoring shall only be upon authorisation by the Union Home Secretary or Home Secretaries of the States/Union Territories.*" (It is unclear whether this is to operate as an overriding provision governing all the other clauses as well).

From the list above, it is very clear that by the terms of their licenses, ISPs are required to maintain extensive logs of user activity for unspecified periods. However, it is unclear, in practice, to what

extent these requirements are being followed by ISPs. For instance, an article in the Economic Times in December 2010 reports:

> The Intelligence Bureau wants internet service providers, or ISPs, to keep a record of all online activities of customers for a minimum of six months. *Currently, mobile phone companies and internet service providers do not keep online logs that track the web usage pattern of their customers. They selectively monitor online activities of only those customers as required by intelligence and security agencies, explained an executive with a telecom company.*[21] (emphasis added)

The same news report quotes Rajesh Chharia, President of the Internet Service Providers' Association of India, as saying, "[a]t present, we only keep a log of all our customers' Internet Protocol address, which is the digital address of a customer's internet connection."

The news report goes on to disclose the ambitious plans of the Intelligence Bureau to "put in place a system that can uniquely identify any person using the internet across the country" through "a technology platform where users will have to mandatorily submit some form of an online identification or password to access the internet every time they go online, irrespective of the service provider." Worryingly, the report goes on to discuss the setting up by the telecommunications department of:

> India's indigenously-built Centralised Monitoring System (CMS), which can track all communication traffic—wireless and fixed line, satellite, internet, e-mails and voice over internet protocol (VoIP) calls—and gather intelligence inputs. The centralised system, modelled on similar set-ups in several Western countries, aims to be a one-stop solution as against the current practice of running several decentralised monitoring agencies under various ministries, where each one has contrasting processing systems, technology platforms and clearance levels.

[21] Jogi Thomas Philip, *Intelligence Bureau wants ISPs to log all customer details*, ECONOMIC TIMES (Dec. 30, 2010, 11:50 AM), http://articles.economictimes.indiatimes.com/2010-12-30/news/27621627_1_online-privacy-internet-protocol-isps.

Although at the time of writing this CMS is not yet fully functional, its launch seems to be imminent and will inaugurate with it, an era of constant and continuous surveillance of all internet users.

2. Provisions under the Information Technology Act, 2000

The IT Act enables government agencies to obtain IP address details from intermediaries, including ISPs, by following a stipulated procedure. In addition, it enjoins intermediaries to co-operate with law enforcement agencies as a part of their due diligence behaviour.

In a parallel and seemingly conflicting move, the IT Act also requires intermediaries to observe stiff Data Protection norms. In the sub-sections that follow, we look at each of these provisions under the IT Act.

(1) Interception and Monitoring of Computer Resources

There are two regimes of interception and monitoring information, under separate sections of the IT Act. Both would seem capable of authorising government agencies access to IP addresses, among other information.

Section 69 deals with "[p]ower to issue directions for interception or monitoring or decryption of any information through any computer resource".[22]

In addition, the Government has been given a more generalised monitoring power under Section 69B, to "monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource."[23] This monitoring power may be used to aid a range of "purposes related to cyber security"[24]. "Traffic data" has been defined in the section to mean "any data identifying or purporting

[22] Information Technology Act (2000), § 69.

[23] Information Technology Act (2000), § 69B.

[24] The Monitoring Rules list 10 'cyber security' concerns for which monitoring may be ordered: (a) forecasting of imminent cyber incidents; (b) monitoring network application with traffic data or information on computer resource; (c) identification and determination of viruses/computer contaminants; (d) tracking cyber security breaches or cyber security incidents; (e) tracking computer resource breaching cyber security or spreading virus/computer contaminants; (f) identifying or tracking of any person who has contravened, or is suspected of having contravened, or being likely to contravene cyber security; (g) undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resource; (h) accessing stored information for enforcement of any provision of the laws relating to cyber security for the time being in force; and (i) any other matter relating to cyber security.

to identify any person, computer system or computer network or any location to or from which communication is or may be transmitted."

Rules have been issued by the Central Government under both these sections[25] which are similar, although with important distinctions. These Rules stipulate the manner in which the powers conferred by the sections may be exercised.

The important difference between the two sections is that while Section 69 provides a mechanism whereby specific computer resources can be monitored in order to learn the contents of communications that pass through such resources, Section 69B by contrast provides a mechanism for obtaining 'meta-data' about all communications transacted using a computer resource over a period of time – their sources, destinations, routes, duration, time, etc., without actually learning the content of the messages involved. The latter type of monitoring is specifically in order to combat threats to 'cyber security', while the former can be invoked for a number of purposes such as the securing of public order and criminal investigation.[26]

However, this distinction is not very sharp – an interception order under Section 69 directed at a computer resource located in an ISP can yield traffic data in addition to the content of all communications. Thus, for instance, if a direction was passed ordering my ISP to intercept "all communications sent or received by Prashant Iyengar", the information obtained by such interception would include a resume of all e-mails exchanged, websites visited, files downloaded, etc. In such a case, a separate order under Section 69B would be unnecessary. An important clue about their relative importance may lie in the different purposes for which each section may be invoked, coupled with the fact that while directions under Section 69 can be issued by officers both at the central and state level, directions under Section 69B can only be issued by the Secretary of the Department of Information

[25] Respectively, the INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARDS FOR INTERCEPTION, MONITORING AND DECRYPTION OF INFORMATION) RULES (2009) and INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARD FOR MONITORING AND COLLECTING TRAFFIC DATA OR INFORMATION) RULES (2009).

[26] Section 69 lists the following grounds for which interception may be ordered: a) sovereignty or integrity of India; b) defense of India; c) security of the State; d) friendly relations with foreign States; e) public order; f) preventing incitement to the commission of any cognisable offence relating to above; or g) for investigation of any offence.

Technology under the Union Ministry of Communications and Information Technology.[27] This indicates that the collection of traffic data by the Government under Section 69B is intended to facilitate the securing of India's 'cyber security' from possible *external* threats – a defence function – while the interception powers under Section 69 are to be exercised for more domestic purposes as aids to police functions.

The Rules framed under Sections 69 and 69B contain important safeguards stipulating, *inter alia*, the following: a) who may issue directions; b) how the directions are to be executed; c) the duration they remain in operation; d) to whom data may be disclosed; e) confidentiality obligations of intermediaries; f) periodic oversight of interception directions by a Review Committee under the Telegraph Act; g) maintenance of records of interception by intermediaries; and h) mandatory destruction of information in appropriate cases.

Although these sections provide powerful tools of surveillance in the hands of the State, these powers may only be exercised by observing the rather tedious procedures laid down. In the absence of any data on interception orders, it is unclear as to what extent these powers are in fact being used in the manner laid down. Certainly, from the instances cited at the beginning of this paper, the police departments in the various states do not seem to need to invoke these powers in order to obtain IP address information from ISPs or websites; this information appears to be available to them merely for the asking. How do we account for this unquestioning pliancy on the part of the ISPs?

In February 2011, Reliance Communications, a large telecom service provider, disclosed to the Supreme Court that over a 150,000 telephones had been tapped by it between 2006 and 2010 – almost 30,000 a year. A majority of these interceptions were conducted based on orders issued from state police departments – whose legal authority to issue them is suspect. New Rules framed under the Telegraph Act in 2007 required such orders to be issued only by a high-ranking Secretary in the Department/Ministry of Home Affairs.[28] The willing compliance by Reliance with the police's

[27] Rule 2(d), INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARD FOR MONITORING AND COLLECTING TRAFFIC DATA OR INFORMATION) RULES (2009).

[28] Telegraph (Amendment) Rules (2007).

requests indicates both their own as well as the police's blithe unawareness about the change in the regime governing tapping. Things seem to have continued just as before through pure inertia.

To return to the question about why ISPs comply with police requests, it is conceivable that this same inertia, and an intuitive confidence both on the part of the police and the ISPs that they would not be made to answer for their disclosures, is what explains the ready and expeditious access that ISPs give police departments to IP address details.

In the next sub-section, we examine intermediary liability rules which require intermediaries to positively disclose personal information to law enforcement authorities.

(2) Data Protection Rules

Section 43A of the IT Act obliges corporate bodies who "possess, deal or handle" any "sensitive personal data" to implement and maintain "reasonable" security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure.

In April 2011, the Central Government notified Rules[29] under section 43A of the Information Technology Act in order to define "sensitive personal information" and to prescribe "reasonable security practices" that body corporates must observe in relation to the information they hold. Since traffic data, including IP address data, is one kind of personal information that ISPs hold, and since all ISPs are "body corporates", these Rules apply to them equally and define the terms on which they may deal with such information.

Rule 3 of these Rules designates various types of information as 'sensitive personal information', including passwords, medical records, etc.[30] Significantly, for the purposes of this paper, IP address details are not included in this list.

---

[29] INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES (2011).

[30] The full list under Rule 3 includes: password; financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above as provided to body corporates for providing service; and any information received under the above by body corporates for processing, stored or processed under lawful contract or otherwise.

Body Corporates are forbidden from collecting any information without prior consent in writing for the proposed usage. Further, Rule 5 states that sensitive personal information may not be collected unless: (a) the information is collected for a lawful purpose connected with a function or activity of the agency; and (b) the collection of the information is necessary for that purpose.

Rule 4 enjoins a body corporate or its representative who "collects, receives, possess [sic], stores, deals or handles" data to provide a privacy policy "for handling of or dealing in user information including sensitive personal information". This policy is to be made available for view by such "providers of information"[31] including on a website. The policy must provide the following details:

(i) Clear and easily accessible statements of its practices and policies;

(ii) Type of personal or sensitive information collected;

(iii) Purpose of collection and usage of such information;

(iv) Disclosure of such information as provided in Rule 6;[32]

(v) Reasonable security practices and procedures as provided under Rule 8.

Rule 6 enacts as a general rule that disclosure of information "by the body corporate to any third party shall require prior permission from the provider of such information". Consent is, however, not required "where disclosure is necessary for compliance of a legal obligation". This is further fortified by a proviso to the rule which stipulates the mandatory sharing of information "without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences." In such a case, the Government agency is required to "send a request in

[31] "Provider of data" is not the same as an individual to whom the data pertains, and could possibly include intermediaries who have custody over the data. I feel this privacy policy should be made available for view generally – and not only to providers of information. In addition, it might be advisable to mandate registration of privacy policies with designated data controllers.

[32] This is well framed since it does not permit body corporates to frame privacy policies that detract from Rule 6.

writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information." The government agency is also required to "state that the information thus obtained will not be published or shared with any other person."[33]

Sub-rule (2) of Rule 6 requires "any Information including sensitive information" to be "disclosed to any third party by an order under the law for the time being in force." This sub-rule does not distinguish between orders issued by a court and those issued by an administrative or quasi-judicial body.

Rule 8 requires body corporates to implement documented security standards such as the international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System".

What is curious about these Rules is that its provisions, particularly those relating to lawful disclosure, appear to go much farther than the limited purpose authorised by Section 43A under which they are framed. Section 43A of the IT Act is intended only to fix liability for the *negligent* disclosure of information by body corporates which results in wrongful loss. It is *not* intended to inaugurate a regime of mandatory disclosure, as the Rules attempt to do. In positively *requiring* body corporates to disclose information upon a mere request by any 'government agency', these Rules attempt to create a parallel, much softer mechanism by which the same information that is dealt with under Sections 69 and 69A and Rules framed under them can be accessed by a far wider range of governmental actors.

Even more curious is the fact that the only legal consequence for the ISP for its negligence in disclosing information to government agencies as stipulated in the Rules is that it exposes itself to possible civil liability from the 'person affected'.[34] Thus, conceivably, if an ISP failed to disclose IP address data of its users to the police at the instance of, say, targets of online financial fraud, they can be sued by the victims of such fraud. With no incentive to assume this ridiculous burden, it is

[33] This is a curious insertion since it begs the question as to the utility of such a statement issued by the requesting agency. What are the sanctions under the IT Act that may be attached to a government agency that betrays this statement? Why not, instead, insert a peremptory prohibition on government agencies from disclosing such information (with the exception, perhaps, of securing conviction of offenders)?

[34] The consequence of disobeying the Rules is that the 'body corporate' is legally deemed not to have observed 'reasonable security practices'. Section 43A penalises such failure if the disclosure causes wrongful loss.

foreseeable that ISPs would hasten to comply with every request for information from a government agency – however whimsically issued.

(3) Intermediary Due Diligence

Section 79 of the IT Act makes intermediaries, including ISPs, liable for third party content hosted or made available by them *unless* they observe 'due diligence', follow prescribed guidelines and disable access to any unlawful content that is brought to their attention.[35] Rules were notified under this Section in April 2011, which defined the 'due diligence' measures they were required to observe.[36]

Accordingly, ISPs are required to forbid users from publishing, uploading or sharing any information that:

(a) belongs to another person and to which the user does not have any right to;
(b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, racially or ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatsoever;
(c) harms minors in any way;
(d) infringes any patent, trademark, copyright or other proprietary rights;
(e) violates any law for the time being in force;
(f) deceives or misleads the addressee about the origin of such messages, or communicates any information which is grossly offensive or menacing in nature;
(g) impersonates another person;
(h) contains software viruses or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting any other nation.

[35] Information Technology Act (2000), § 79.

[36] INFORMATION TECHNOLOGY (INTERMEDIARIES GUIDELINES) RULES (2011).

Upon being notified by any 'affected person' who objects to such information in writing, the ISP is required to "act within thirty six hours and where applicable, work with [the] user or owner of such information to disable such information."[37]

Further, "when required by lawful order", the ISP, website or any other intermediary:

> shall provide information or any such assistance to Government Agencies that are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

The same attempt at subversion of Sections 69 and 69B, as discussed in the previous sub-section under the Data Protection Rules, is visible here. Failure to observe these 'due diligence' measures – including disclosure of IP address details – would expose ISPs and web services like Google and Facebook to civil liability under Section 79, a risk they would not be likely to or lightly wish to assume.

3. Police Powers of Investigation

Apart from the provisions under the IT Act, to what extent are the police in India empowered under the Code of Criminal Procedure to simply requisition information – including IP addresses of suspects – from ISPs and websites? In the course of routine investigation into other offences, the police have wide powers to summon witnesses, interrogate them and compel production of documents. Can these

[37] The easily-affronted have thus been provisioned with a cheaper, swifter and more decisive means of curtailing free speech, where courts in India might have dithered ponderously instead. Or they might not have. At the time of writing this, an obscure court in Silchar, Assam, issued an ex-parte injunction prohibiting the online publication of a highly-acclaimed biopic about Arindam Chaudhuri – a self-proclaimed 'management guru' who has gained notoriety in India due the questionable nature of a management institute that he runs. The choice of this particular court as the venue to file the suit, rather than one in New Delhi where both the plaintiff and the publisher reside, coupled with Chaudhuri's consistent success in obtaining such plenary gag-orders from this judge against any content he deems unflattering to himself, strongly suggests foul-play. Although this is not a typical case, it does caution against placing too much optimism on supposed judicial restraint and conservativeness. *IIPM's Rs 500-Million Lawsuit against The Caravan*, THE CARAVAN (July 1, 2011), http://caravanmagazine.in/Story/950/IIPM-s-Rs500-million-lawsuit-against-The-Caravan.html.

powers be invoked to obtain IP address information? Are ISPs and websites somehow immune from complying with these requirements?

Section 91 of the Code of Criminal Procedure empowers courts or police officers to call for, by written order, the production of documents or other things that are "necessary or desirable" for the purpose of "any investigation, inquiry, trial or other proceeding under the Code".

Sub-section (3) of this Section, however, limits the application of this power by exempting any "letter, postcard, telegram, or other document or any parcel or thing in the custody of the postal or telegraph authority." Such documents can only be obtained under judicial scrutiny by following a more rigorous procedure laid down in Section 92. Under this Section, it is only if a "District Magistrate, Chief Judicial Magistrate, Court of Session or High Court" is of the opinion that "any document, parcel or thing in the custody of a postal or telegraph authority is...wanted for the purpose of any investigation, inquiry, trial or other proceeding under this Code" that such document, parcel or thing can be required to be delivered to such Magistrate or Court.

However, the same Section empowers lesser courts and officers such as "any other Magistrate, whether Executive or Judicial, or ... any Commissioner of Police or District Superintendent of Police" to require "the postal or telegraph authority, as the case may be ...to cause search to be made for and to detain such document, parcel or thing" pending the order of a higher court.

Section 175 of the Cr.P.C. makes it an offence for a person to intentionally omit to produce a document which he is legally bound to produce. In case the document was to be delivered to a public servant or police officer, such omission is punishable with simple imprisonment of up to 1 month, or with fine up to five hundred rupees, or both. If the document was to be delivered to a Court of Justice, omission could invite simple imprisonment up to 6 months, with or without a fine of one thousand rupees.

In the context of our discussion on IP addresses, the following questions emerge:

1) Are ISPs "telegraph authorities" such that the police are ordinarily prohibited from requisitioning information from them without obtaining orders from a court?

2) Similarly, are webmail and social networking sites "telegraph or postal authorities" such that securing information from them requires following of the special procedure laid down in Section 92?

Section 3(6) of the Indian Telegraph Act, 1885 defines "telegraph authority" as "the Director General of [Posts and Telegraphs], and includes any officer empowered by him to perform all or any of the functions of the telegraph authority under this Act."[38] This would seem to exclude all private sector ISPs from the definition, presumably opening them up to ordinary summons issued under Section 91.

However, Section 3(2) defines a "telegraph officer" to mean "any person employed either permanently or temporarily in connection with a telegraph established, maintained or worked by [the Central Government] *or by a person licensed under this Act*".[39] Under this section, employees of private ISPs such as Airtel would also be regarded as "telegraph officers" and if we can extend this logic, with some interpretative work, the ISPs themselves might be regarded as "telegraph authorities". In the absence of definite rulings by the judiciary on this question, however, the ordinary presumption would be that private ISPs are not "telegraph authorities" and are answerable, like all private companies, to requisitions made under Section 91.

This leaves open the question of whether a government company like BSNL would count as a 'telegraph authority'. If it is, then it would put internet communications conducted through BSNL on a more secure footing than those conducted through other ISPs. As things stand, however, it appears that BSNL seems to be extending its co-operation to the police in tracking mischief online,[40] in the same manner as other ISPs.

---

[38] Indian Telegraph Act (1885), § 3(6).

[39] Indian Telegraph Act (1885), § 3(2).

[40] *See* ALI, *supra* note 9 ("During investigations, the police browsed through several service providers and finally zeroed in on BSNL, which helped them trace the sender's IP address to someone called 'Manoj Gupta' in Gurgaon. A team of policemen were sent to Gurgaon but the personnel found out that Manoj Gupta was [a] fictitious name which the teenager was using in his IP address. The police arrested the accused as well as seized the hardisk [sic] of his personal computer."). *See also* Teresa Rehman, *A Case For Fools?*, TEHELKA (Oct. 10, 2008), http://www.tehelka.com/story_main40.asp?filename=Ws181008case_fools.asp ("The state police reportedly traced the email to the cyber café through its IP address. "We traced the email to a BSNL line. The BSNL has a cell in Bangalore to track such details. They traced the number to that particular cyber café in Shillong," S.B. Singh, IGP (special branch), Meghalaya police told TEHELKA").

The second question is relatively more straightforward. The definition of "post office" in Section 2(k) of the Indian Post Office Act, 1898 restricts its meaning to "the department, established for the purposes of carrying the provisions of this Act into effect and presided over by the Director General [of Posts and Telegraphs]". Despite their primary functions as e-mail providers, it seems unlikely that any magistrate would interpret webmail providers like Hotmail and Google as "postal authorities" so as to be immune from police summonses under Section 91. Such an interpretation would, nevertheless, be in keeping with the spirit of the postal exemptions, since these sections seem to be aimed at requiring judicial oversight before the privacy of communications may be disturbed. It would be fitting for an amendment to be introduced to the Code of Criminal Procedure to update these sections in line with new technological developments.

Before parting with this sub-section, it must be asked whether the procedure under the IT Act or the Code of Criminal Procedure must be followed. Section 81 of the IT Act unequivocally declares that the Act is to have overriding effect "notwithstanding anything inconsistent therewith contained in any other law for the time being in force." This seems to suggest that at least with respect to the interception of electronic communications and obtaining traffic data, the provisions of the Code of Criminal Procedure would be overridden by the procedure laid down by the Rules under the IT Act. The evidence from the practice of the Indian police routinely obtaining IP address from web service providers and ISPs seems to suggest that the IT Act has not been invoked in these transactions. This is a trend that is likely to continue until its legality is questioned in a court of law.

4. Subscriber Contracts with Web Service Providers

In addition to statutory provisions mandating the disclosure of IP address information, such disclosure may also be permissible by the terms under which individual websites provide their services. Two examples would suffice here:

Google's privacy policy which governs its full range of services, from its popular search service to Gmail, as well as the groups and blogging services, states that the company will disclose personal information *inter alia if*:

> [w]e have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable

> governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.[41]

Information collected by Google includes server logs which include the following information: "your web request, your interaction with a service, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser or your account."[42]

Similarly, social networking site Facebook contains an equally expansive 'lawful disclosure' clause in its Privacy Policy,[43] which states that the company will disclose information:

> [t]o respond to legal requests and prevent harm. We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.

Information collected by Facebook includes information about the device (computer, mobile phone, etc.), the browser type, the location and IP address, as well as the pages visited.[44]

---

41 *Privacy Policy*, GOOGLE (Oct. 3, 2010), http://www.google.com/policies/privacy/archive/20101003/.

42 *Id.*

43 *Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last visited June 28, 2011).

44 *Ibid.*

Examples of such clauses abound and it would be fair to assume that almost every corporate website one visits has analogously worded terms of service permitting 'lawful disclosure'. This contractual backdoor negatives any expectation of absolute privacy of IP address details that one might mistakenly have harboured.

Conclusion

IP addresses have proven to be a dependable way for the police in India to track down a range of cyber-criminals – from financial frauds, to vengeful spurned-lovers, to blackmailers and terrorists. The novelty of 'cyber crimes', as well as the relative high-tech ease of their resolution, makes for attractive press and offers an inexpensive way for police departments to accrue some credibility and goodwill for themselves. So long as the police track down *genuine* culprits, the question of privacy violations will necessarily remain suppressed since, in the words of the Supreme Court, "*the protection [of privacy] is not for the guilty citizen against the efforts of the police to vindicate the law*."[45] However, it is the possibility of an increase in egregious cases such as those of Lakshmana Kailash, mentioned above, wrongfully jailed for 50 days on account of a technical error, that reveals the pathologies of the unchecked system of IP address disclosure that prevails today.

Legal regimes in the West have largely been indecisive about whether to characterise the maintenance of IP address logs as handmaids for Orwellian thought-policing, or merely as implements that aid the apprehension of cyber criminals who have no legitimate expectation of privacy. Their laws typically come with procedural safeguards such as mandatory notices to affected persons[46] and judicial review, which greatly mitigate the severity of these disclosures when they do occur.

Far from incorporating such safeguards, the various layers of Indian law create an atmosphere that is intensely hostile to the withholding of such information by ISPs and intermediaries. Overlapping layers of regulation between the Telegraph Act and the IT Act, and the conflict among various Rules under the IT Act have created a climate of such indeterminacy that immediate compliance with even

---

[45] R. M. Malkani v. State of Maharashtra, AIR 1973 SC 157.

[46] *E.g.*, 18 U.S.C. § 2703 (1997) provides for mandatory notice in case of wiretapping with a provision of 'delayed notice' where an 'adverse result' is apprehended such as (A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

the most capricious of information demands by any government agency is the only prudent recourse for ISPs and other intermediaries. The DoT has issued a circular requiring the registration of public and domestic wifi networks to facilitate greater precision in tracking individuals behind IP addresses.[47] For the same purpose, new Cyber Café Rules under the IT Act require extensive registers and logs to be maintained that track the identity of every user and the websites they have visited.[48] And if the full ambitions of the Unique Identity Numbering Scheme and the Centralised Monitoring System are realised, we will shortly be headed for exactly the kind of persistent surveillance society that Orwell wrote so fondly about.

The Indian judiciary, which could have played a counterbalancing role to the legislature's apathy towards privacy and the executive's increasingly totalitarian tendencies, has so far not risen to the challenge. The Supreme Court has repeatedly condoned the obtaining of evidence through illegal means,[49] and this has rendered the requirement of adherence to procedural due process by the police merely optional. This guarantee of judicial inaction in the face of executive illegality will be the biggest stumbling block to the securing of privacy – despite the occasionally good intentions of the legislature.

So, in the absence of a general assurance of privacy of our internet communications, where does one look to for hope? I would venture to suggest that there are four sources of optimism:

a) Notwithstanding the iron determination of the Central Government to install a panoptic communication surveillance system, the realisation and smooth functioning of these technocratic fantasies will depend on the reconfiguration of the relative powers of various

---

[47] Letter from Department of Telecommunications, Ministry of Communications & IT, Government of India to All Internet Service Providers (Feb. 23, 2009), http://www.dot.gov.in/isp/Wi-%20fi%20Direction%20to%20ISP%2023%20Feb%2009.pdf . Internationally, this does not appear to be an uncommon move. *See* Carolyn Thompson, *Innocent Man Accused Of Child Pornography After Neighbor Pirates His WiFi*, HUFFINGTON POST (Apr. 24, 2011, 10:49 AM), http://www.huffingtonpost.com/2011/04/24/unsecured-wifi-child-pornography-innocent_n_852996.html ("In Germany, the country's top criminal court ruled last year that Internet users must secure their wireless connections to prevent others from illegally downloading data. The court said Internet users could be fined up to $126 if a third party takes advantage of their unprotected line, though it stopped short of holding the users responsible for illegal content downloaded by the third party.").

[48] INFORMATION TECHNOLOGY (GUIDELINES FOR CYBER CAFE) RULES (2011).

[49] *See* State Of Maharashtra v. Natwarlal Damodardas Soni, AIR 1980 SC 593.

ministries at the central level – chiefly, the Ministry of Communications and Information Technology and the Home Ministry – and between the Centre and the State. One can rely, one feels, on the unwillingness of various ministries to cede their powers to forestall, or at least delay or diminish the execution of this project. The success of the technology, in other words, is not as much in doubt as is the success of the politics. Privacy will triumph in this 'failure' of politics. I advance this point naively and with only the slightest sense of irony.

b) Another ironic point: I suggest the ingenious and very Indian phenomena of inefficiency and ignorance as robust privacy safeguards. How does one account for the fact that despite heavily worded and repeated invocations of disclosure requirements in the ISP licenses for almost a decade, it was not until December 2010 that the Home Ministry tentatively suggested to ISPs that IP records must be kept for a minimum of six months?[50] This, despite the fact that the ISP license itself requires that such records be kept for one year. How does one explain the unanimous blinking astonishment of the industry at this suggestion, other than they *expected* never to have to implement it*?* How else, similarly, does one explain the fact that the extensive logs that cyber café owners are required to maintain about their clientele are seldom checked?[51] Or that a year after the DoT's circular forbidding open wifi routers, 17% of wireless connections in Mumbai alone were reported 'unsecured'? In India, it seems to be an unstated element of the business climate that one can reliably depend on the non-enforcement of contractual clauses. Sometimes, this inefficiency on the part of the State has inadvertent privacy-preserving effects.

c) The power of the state to rely on IP addresses depends on the availability of global internet behemoths such as Microsoft, Google, Facebook and Yahoo, who are vulnerable to bullying in order to maintain their transnational empires. In each of the success stories mentioned at

[50] MCINTYRE, *supra* note 3, at 5.

[51] Shalabh Manocha, *Cops no more interested in checking cyber cafes*, TIMES OF INDIA (Aug. 3, 2009, 1:26 AM), http://articles.timesofindia.indiatimes.com/2009-08-03/lucknow/28172232_1_cyber-cafe-proper-records-ip-address ("The cyber cafe owners claim that the registers which they maintain are seldom checked by the police. "I maintained the records properly which included recording of the name and address of the visitors and a photocopy of their identification proofs but not even once any cop had checked [sic] my records," said Rajeev, a cyber cafe owner in Aliganj. "It is this carelessness on the part of cops that gives those not maintaining proper records to [sic] carry on their business without any fear of the law," he added.").

the start of this paper, IP address details were obtained from one of the big companies named, from which the lesson that emerges is that our ability to retain our anonymity will depend on our ability to find smaller, non-Indian substitutes who have nothing to fear from Indian authorities. In June 2010, for instance, the Cyber Crime Police Station, Bangalore sent a notice under Section 91 of the Cr.P.C. to the manager of BloggerNews.Net (BNN) seeking the IP address and details of a user who had allegedly posted "defamatory comments" on BNN about an Indian company called E2-Labs. The manager of BNN bluntly refused to comply stating: "our policy is not to give out that information, BNN holds people's privacy in high esteem."[52] The lesson here is that in the future, the ability of Indians to preserve their online 'privacy' and freedom of speech will depend on their being able to find sufficiently small overseas clients to host their speech. Conflict of Laws, rather than domestic legislation, is a more reliable guarantor of privacy.

---

[52] Simon Barrett, *Blogger News Censored In India*, BLOGGER NEWS NETWORK (July 12, 2010), http://www.bloggernews.net/124890.