GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

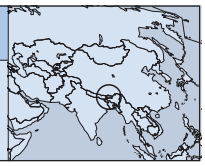
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

NEPAL

Somebody's watching me?



Development Knowledge Management and Innovation Services Pvt. Ltd.
Kishor Pradhan
www.dekmis.com

Introduction

Located in South Asia, Nepal is a relative latecomer as a republic in democratic circles. After more than a decade of insurgency, the interim constitution promulgated in 2007, which is still in force, paved the way for the first constituent assembly election (CAE) in 2008. The constituent assembly formed from this abolished the more than century-old monarchy. Nepal has been in the process of writing a new constitution since 2008. After the second CAE in 2013 and the formation of the second assembly, it is hoped that in a year or two the people of Nepal will finally have the pleasure of a new constitution and a stabilisation of the envisioned federal republic of Nepal.

According to the latest Nepal Telecommunication Authority (NTA) Management Information System Report published in February 2014, Nepal, with its population of 26,494,504,[1] has an 84.77% telephone penetration rate. The data shows there is a 74.97% mobile penetration rate among telephone users. At the moment, Nepal has an internet penetration rate of 28.63%, with 7,585,761 users.[2]

The OpenNet Initiative (ONI) reported that Nepal had little or no internet censorship in 2007. ONI conducted testing from October 2006 through January 2007 on six Nepali ISPs,[3] and the tests revealed no evidence of filtering.[4]

However, four years ago, September 2010 was a dark period for netizens[5] in Nepal who until then had enjoyed a free internet to its fullest extent. The authorities, out of the blue and citing the reasons that there had been an increase in crime and anti-social activities using the internet, formed a special central investigation bureau that started clamping down on internet service providers (ISPs) to track the misuse of the internet by their subscribers.[6]

In 2011 the ISPs were told by the authorities to monitor their subscribers' activities and those who failed to do so were jailed. Since then the government has been monitoring the browsing details of high-bandwidth subscribers. The NTA has directed ISPs to provide information on all subscribers who use a bandwidth of 1 Mbps or more.[7] The Nepal police work closely with NTA technicians now in a joint task force to scan web details of users so that they can identify voice over internet protocol (VoIP)[8] racketeers.

The NTA further made it mandatory for ISPs to install filtering software to block websites that are "obscene, seductive and corrupt social morals". Any content that threatens "religious harmony, national security, and goes against values and beliefs of the state" was deemed objectionable enough to be blocked.[9] Under pressure, the ISPs have been providing the police with Multi Router Traffic Grapher (MRTG)[10] data of subscribers for network traffic monitoring since 2011.

Of late Nepali netizens cannot help feeling that "somebody's watching me"[11] while using the internet or communicating by some other technological means.

Policy perspectives

In order to assess the policy perspectives regarding privacy rights and mass communications

1 www.cbs.gov.np

2 www.nta.gov.np/en/mis-reports-en

3 According to the Internet Service Provider Association of Nepal there are currently 43 internet service providers and nine VSAT network service providers in Nepal. www.ispan.net.np/registered-isp-list

4 https://opennet.net/research/profiles/nepal

5 The term netizen is a portmanteau of the English words internet and citizen. It is defined as an entity or person actively involved in online communities and a user of the internet, especially an avid one. en.wikipedia.org/wiki/Netizen

6 Pradhan, K. (2010, September 20). Can internet be muzzled in Nepal? *Nepalnews.com*. www.nepalnews.com/index.php/guest-column/9294-can-internet-be-muzzled-in-nepal

7 Mahato, R. (2011, July 22). Surfing under surveillance. *Nepali Times*. nepalitimes.com/news.php?id=18395

8 VoIP is illegal in Nepal, although netizens use Viber, Skype, Tango and other internet-based voice communication services.

9 Mahato, R. (2011, July 22). Op. cit.

10 The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network links. MRTG generates HTML pages containing PNG images that provide a live visual representation of this traffic. oss.oetiker.ch/mrtg/doc/mrtg.en.html

11 Somebody's Watching Me was the title of a song by R&B artist Rockwell, released on the Motown label in 1984. The song's lyrics relate the narrator's paranoid fear of being followed and watched. en.wikipedia.org/wiki/Somebody's_Watching_Me

surveillance in Nepal, primarily three legal or policy provisions need to be considered.

In Article 22 of the Constitution of the Kingdom of Nepal 1990, the right to privacy was addressed as a fundamental right for the first time. The right to information was also included in the constitution. Later, the right to privacy was retained in the 2007 interim constitution, which remains in force today. Article 28 of the interim constitution states: "Except in circumstances as provided by law, the privacy of the person, residence, property, document, statistics, correspondence, and character of anyone is inviolable." However, there is no government authority to receive complaints regarding violations of privacy rights, although people may submit applications and reports concerning violations of their privacy rights to the National Human Rights Commission (NHRC). It is also possible to file a case in the Nepalese courts regarding violation of the right to privacy.[12]

In Chapter 2 of The Right to Information Act of 2007 (RTI Act 2007), entitled "Right to Information and Provisions Regarding the Flow of Information", Article 3 deals with the right to information and states: "Every citizen shall, subject to this Act have the right to information and every citizen shall have access to the information held in the public Bodies."[13] The right to information is however stipulated by defining the parameters of the information that can be accessed; notwithstanding anything provided for in Sections (1) and (2) of the RTI Act 2007, the information held by a public body on certain subject matters cannot be disseminated.[14]

The Nepal Electronic Transaction Act of 2008[15] serves as the cyber law in Nepal. In general it establishes legal provisions on the "dos and don'ts" for using ICTs such as computers and the internet, and on the nature of content circulated online. It provides for the official and legal application of electronic transactions such as digital signature and certification, but is silent about how privacy will be protected. Nevertheless, the cyber law has critically empowered the authorities more when it comes to protecting the privacy rights of people.

Somebody's watching me?

When the authorities clamped down on ISPs in 2010, they said that VoIP is illegal in Nepal but that many of the public communications service providers were and still are rampantly using the internet to provide relatively low-cost calls. The authorities argued that, due to the illegal use of the internet for online calls which bypassed the NTA, it was losing billions of rupees every year.[16] Who was responsible for this was not clear, however, as the ISPs countered that they provide the internet bandwidth to their subscribers – who *could* be public communications service providers – but they cannot really monitor or regulate what the internet bandwidth gets used for.

Further, the authorities claimed that the internet was used for criminal activities, as no record can be traced of internet calls. At the same time there were increasing cases of "objectionable" content being posted on websites from Nepal.

Rubeena Mahato, reporting on the tougher controls imposed by the NTA in 2010, emphasised that "MRTG data only allows monitoring the browsing patterns of users, but could be a stepping stone for the government to introduce censorship and intrude on private correspondence in the future."[17]

Measures taken by the authorities in Nepal for specific communications surveillance of criminal and objectionable activities are reasonable. But the monitoring of MRTG data entails mass communications surveillance. Mass communications surveillance entails surveillance of personal data and metadata, or what the International Principles on the Application of Human Rights to Communications Surveillance (IPAHRCS) – adopted through a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and regulation in July 2013 – defines as "protected information". Information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public should be considered to be "protected information", and should accordingly be given the highest protection in law.[18]

12 Privacy International. (2012). *Nepal*. https://www.privacyinternational.org/reports/nepal

13 www.moic.gov.np/acts-regulations/right-to-information-act.pdf

14 As per the RTI Act 2007, the subject matters on which information cannot be disseminated by a public body include information which seriously jeopardises the sovereignty, integrity, national security, public peace, stability and international relations of Nepal; which directly affects the investigation, inquiry and prosecution of a crime; which seriously affects the protection of economic, trade or monetary interest or intellectual property or banking or trade privacy; which directly jeopardises the harmonious relationship among various castes or communities; and which interferes with the individual privacy and security of body, life, property or health of a person.

15 www.tepc.gov.np/uploads/files/12the-electronic-transaction-act55.pdf

16 In July 2014, the exchange rate was approx. 96 Nepali rupees per 1 USD.

17 Mahato, R. (2011, July 22). Op. cit.

18 https://en.necessaryandproportionate.org/text

Communications surveillance and violation of privacy rights are said to be increasing in Nepal. This perspective is corroborated by a recent incident on 18 April 2014, when Vinaya Kasaju, former chief commissioner of the National Information Commission (NIC), updated his Facebook status:

> Dear FB friends, I cannot write this message in Nepali, because police personnel from Aparadh Anusandhan Mahasakha,[19] Hanumandhoka, have taken away my desktop computer. They came at about 3:30 p.m. They showed me their identity card. I asked for letter. They said we have come with an order of boss. If you don't come with us, we must force you. I followed them to their van. On half way they talked with their chief and stopped the van. Waited for about half an hour in front of Radiant Academy, Sanepa, then they brought me back home. They also got a written receipt from us that Ganga, my wife, received. They took our photos. Ganga took photos of them and of their receipt. They mentioned that they have taken my computer. But we do not have hard copy of receipt, only photo which I'm trying to put here. Don't I have right to know why I was arrested, even for an hour? I am deprived of my communication tool. Who will save our RTI?

The next day Vinaya posted the following:

> Hegemony of some big media house is increasing in our country too. Dil Sobha was reported as criminal running sex trade. Yesterday one big media covered Kanak Dixit as if he has done a big scandal. They don't wait for investigation report or court decision. I came to know unofficially, that a big media boss complained against my website www.cmr.org.np charging that he is losing the money from Google Ads. What a shame. There is no ad in my website. It is not difficult to find where Google Ads money is going. Has the media boss ever paid tax of that income to the government? I want my computer back as soon as possible safely, without loss or manipulation or theft of any data/file. As the former chief information commissioner, as a media consultant and as an author there are files of national importance and my resources for study and writing. There are many such files about which I can tell only to concerned authority. I hope and request to return my computer safely.[20]

In all this Vinaya concludes that the cyber crime authorities in Nepal took action against him wrongly, which was the result of the lack of capacity of the authorities in tracking or locating the actual culprit. He concluded, "The capacity of the authorities to deal with and investigate cyber crimes is lacking in Nepal. Their capacity needs to be built to handle cyber crime issues, so that the real criminals are caught and innocent people are left alone."[21]

The ordeal Vinaya went through was a gross violation of his privacy rights. The authorities, without any warrant and on the basis of an informal complaint to a senior police authority by a powerful media mogul, violated his privacy rights.

It is not that the authorities or any other citizen in Nepal do not have rights to information. As established by the Right to Information Act, an institution or an individual is entitled to have access or the right to information, but by following a proper procedure. The NIC, formed under the Act, manages right-to-information cases. After receiving a request for information and verifying the authenticity, the NIC decides on the ensuing action. And this is applicable to government authorities, such as police departments, too.

The issue is the juxtaposition and limitation of the right to privacy, right to information and communications surveillance. As the legality principle of the IPAHRCS states:

> Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which means a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technology changes, laws that limit the right of privacy should be subject to periodic review by means of a participatory legislative or regulatory process.[22]

Given the rapid changes in the communications landscape, it is about time that the authorities in Nepal revisit the current right-to-privacy legal provisions, those that deal with the right to information, as well as mass communications surveillance policies and practices. The authorities should be able to reassure citizens and netizens alike that their privacy is not intruded on when communicating, and

19 In English, Crime Investigation Department.

20 https://www.facebook.com/vinaya.kasajoo?fref=ts

21 Personal conversation with Vinaya Kasaju.

22 International Principles on the Application of Human Rights to Communications Surveillance. https://en.necessaryandproportionate.org/text

make them not feel that "somebody's watching me" when communicating privately, socially, professionally or officially.

Conclusions and action steps

The conclusions that can be drawn from the Nepal experience so far are two-fold. On the one hand it can be asked, how is the right to privacy going to be protected by the authorities in a changed communication landscape? On the other hand, given the imperative of communications surveillance for national security and crime control, how is it not going to be intrusive?

These juxtaposed perspectives urgently call for the authorities to revisit the issues of the right to privacy and the imperative of communications surveillance and find a balanced middle path that can uphold both. In this context, the following action steps can be suggested.

- The authorities need to revisit the policies or laws related to the right to privacy and reformulate them in the changed context of the ways people communicate or access information or process and maintain personal data.
- Regarding the laws or policies for communications surveillance, the authorities should formulate regulations which distinctly address the issues of internet censorship and communications surveillance.
- Communications surveillance, whether mass communications surveillance or specific communications surveillance, needs to be distinguished by law or policy and regulated accordingly, following a standard legal procedure.
- Civil society, especially rights-based organisations, should be more engaged in Nepal on lobbying the authorities to recognise and protect the right to privacy and the right to communication, without being under surveillance.
- International rights organisations and donors working on the right to privacy related to communications surveillance should provide technical assistance to the government and civil society (including the media) in developing countries like Nepal, in order to build their capacity for addressing and managing the issues of privacy and communications surveillance in line with international principles or conventions.