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

INDIA

Communications surveillance, human rights and freedom of expression in India

Digital Empowerment Foundation (DEF)
Ritu Srivastava
www.defindia.org

Introduction

The internet is a key tool to exercise the right to freedom of expression. It not only allows us to exercise the right to receive information, knowledge, ideas and opinions, but also allows us to exercise the right to express these – be it in the form of video, audio or writing. Used as a publishing and communication tool, it enables millions around the world to communicate instantly, gives the common citizen a voice among an audience of millions, and serves as a huge multimedia library of information. One definition says "the internet is as diverse as human thought."[1]

As access to the internet becomes more diverse, including information on prominent social issues is becoming important. United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression and Opinion Frank La Rue underlined in his report submitted to the Human Rights Council (HRC) regarding the unique and transformative nature of the internet that it not only enables individuals to exercise their right to freedom of expression and opinion, but also allows them to exercise other human rights and to promote the progress of society as a whole.[2] It has been proven that technological advances have been powerful tools for democracy by giving access to all. However, data mining by intelligence agencies blurs lines between legitimate surveillance and arbitrary mass surveillance by governments nationally and internationally.

La Rue also emphasised how government and corporate surveillance are undermining freedom of expression. His report states: "Freedom of expression cannot be ensured without respect to privacy in communications. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other."[3]

His report established the connection between freedom of expression and privacy in communications and called for global attention to the widespread use of surveillance mechanisms by various governments that are violating human rights, such as the right to privacy and freedom of expression. It also makes the point that privacy is a fundamental human right, and is important for democratic society to maintain its human dignity. Furthermore, the right to privacy reinforces other rights, such as freedom of expression and information, and freedom of association, also recognised under human rights law.[4] However, it is difficult to define exactly what the right to privacy entails. Privacy can be seen from two perspectives – it depends on the type of information we share or the sides of our lives that we want to keep private, and whether or not the information is in the public interest.

Governments worldwide have continued to justify their engagement in wide-ranging surveillance programmes – often at the very limits of the law – arguing national security concerns. While India is the world's largest democracy and is said to be protecting freedom of speech through its laws and constitution, freedom of expression online is increasingly being restricted in the country. Justifications given for these restrictions are the problem of defamation and the need to maintain national security and peace in society.

This became evident when the Indian government announced the start of the Centralised Monitoring System (CMS) in 2009, a programme to monitor telecommunications in the country. In 2013, Minister of State for Communications and Information Technology Milind Deora initiated the rollout of CMS across India. This report analyses how government surveillance works in India, and how government and private organisations are accessing individuals' online data, which is a threat to freedom of expression.

1 ACLU v. Reno, 929 F. Supp. 824, 830-849 (ED Pa. 1996) at 842 (District Court Opinion)

2 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

3 Ibid.

4 Universal Declaration of Human Rights, Article 12; United Nations International Convention on the Protection of the Rights of All *Migrant Workers* and Members of Their Families, Article 14.

Communications surveillance laws in India

The term "communications surveillance" encompasses the monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information which arises from, reflects or is about a person's communications in the past, present or future. With more and more people accessing the web, the internet user base in India reached 243 million[5] in 2014. This medium not only enables users to exchange information and deliver services, but also allows political discourse. Platforms like Facebook and Twitter and blogs make it easy for people to communicate and reach a vast audience.

Unlike PRISM, the United States surveillance programme that captured the world's attention ever since whistleblower Edward Snowden leaked details of global spying to *The Guardian* and *Washington Post*, India silently launched the CMS to monitor internal communications in 2013. The system cost USD 75 million, and will allow the government to access all digital communications and telecommunications in the country.

Since independence, laws in India have prohibited the unlawful interception of communications. For example, Section 26 of the India Post Office Act, 1898 allows the interception of post for the "public good" only. According to this section, this power may be invoked "on the occurrence of any public emergency, or in the interest of the public safety or tranquillity."[6] The section also says that "a certificate from the State or Central Government" is required that would serve as conclusive proof as to the existence of a public emergency, or to show that the interception is in the interest of public safety or peace. Similarly, Section 5(2) of the Telegraph Act, 1885 also authorises the interception of messages, but only a) in the event of a public emergency, or in the interest of public safety; and b) if it is necessary or expedient to do so 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.[7]

In the case of Hukam Chand Shyam Lal vs. Union of India and Others,[8] the Supreme Court of India interpreted the meaning of "public emergency". The court considered "public emergency" merely as an "economic emergency", and justified surveillance under this section unless it raised problems relating to the matters indicated in the section. The court also considered another qualifying term, "public safety", as "security of the public or their freedom from danger".

Two separate sections of the Information Technology Act 2000 deal with interception and monitoring of information. Section 69 deals with the "[p]ower to issue directions for interception or monitoring or decryption of any information through any computer resource".[9] Section 69B deals with the "monitor[ing] and collect[ion] of traffic data or information generated, transmitted, received or stored in any computer resource". This monitoring power can be used for cyber security purposes.[10] The term "traffic data" has been defined under Section 69B as "any data identifying or purporting to identify any person, computer system or computer network or any location to or from which communication is or may be transmitted."

Surveillance is not only limited to individual monitoring. Section 67C of the Information Technology Act deals with "intermediaries", and requires them to maintain and preserve certain information under their control for a minimum of three months. Failure to do this is punishable with imprisonment for up to three years and a fine under Section 67 C(2). Section 79 of the Information Technology Act[11] provides immunity from liability for intermediaries for third party content that is hosted by them. However, in 2011, the Ministry of Information and Technology issued two more sets of rules under this Act – firstly to govern intermediaries such as internet service providers (ISPs) and web platforms, and secondly to govern cybercafés. Both of these sets of

5 Times of India. (2014, January 29). India to have 243 million internet users by June 2014: IAMAI. *Times of India*. timesofindia.indiatimes.com/tech/tech-news/India-to-have-243-million-internet-users-by-June-2014-IAMAI/articleshow/29563698.cms

6 The Indian Post Office Act, 1898. www.indiapost.gov.in/Pdf/Manuals/TheIndianPostOfficeAct1898.pdf

7 The Indian Telegraph Act, 1885. http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf

8 AIR 1976 SC 789, 1976 SCR (2)1060, (1976) 2 SCC 128.

9 Section 69 of the Information Technology Act. www.chmag.in/article/jan2012/powers-government-under-information-technology-act-2000

10 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 resources; (c) identification and determination of viruses/computer contaminants; (d) tracking cyber security breaches or cyber security incidents; (e) tracking computer resources breaching cyber security or spreading viruses/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 investigation of the concerned computer resource as a part of an investigation or internal audit of information security practices in the computer resource; (h) accessing stored information for enforcement of any provisions of the laws relating to cyber security in force at the time; (i) any other matter relating to cyber security.

11 sflc.in/information-technology-act-and-rules-time-to-change

rules severely diminish the freedom of expression of citizens and their right to privacy.

India, which is poised to be one of the biggest markets for video surveillance, registered growth of 20% in this regard in the last quarter of 2013. The Delhi International Airport has installed 3,700 IP surveillance cameras,[12] the "largest single installation of an IP video system anywhere in India." Both the government and private businesses have enthusiastically embraced CCTV technology, including in municipalities, police departments, airports, banks, schools and supermarkets. Despite the fact that CCTV cameras were installed to tackle terrorism and crime, there are no laws that govern their deployment or use in India. The closest law applies to electronic voyeurism and is contained in Section 66E of the Information Technology Act, which punishes the "capturing, publishing and transmission" of images of any person in a "private area" without their consent, "under circumstances violating the privacy" of that person. This offence is punishable with imprisonment of up to three years or a fine of up to two lakhs rupees (approx. USD 3,000).

Moreover, in 2011, the government expanded its internet surveillance in cybercafés, the primary access points for rural villagers. Users now need to provide their identity card for accessing cybercafés. Requesting this kind of user data is questionable when it is used for prosecuting free speech online and stifling political criticism. India is also one of the worst offenders for takedowns, as well as for requests for user information. The Google Transparency Report shows that on requests for user information it is ranked after the US only.[13]

At the end of 2012, most of the major telecom companies in India agreed to grant the government real-time interception capabilities for the country's one million BlackBerry users.[14] The government is also constantly requesting major web companies to set up their servers in India in order to monitor local communications.

Freedom of expression and communications surveillance

The Constitution of India guarantees freedom of expression under its Article 19(1). However, Article 19(2) restricts the exercise of freedom of expression. Article 19(2) can be enforced by the state in the interest of the sovereignty and integrity of the state, the security of the state, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.[15] The constitution does not include a freestanding right to privacy. However, the Supreme Court of India has read the right to privacy in Article 21 of the constitution – the right to life and liberty. It states, "No person shall be deprived of his life or personal liberty except according to procedure established by law."[16] Considering the right to freedom of expression and the right to privacy, the fundamental question is the balance between the two.

For the last few years, a comprehensive Privacy Bill has been under discussion in India, although it has still not been adopted by the government. A draft dated 19 April 2011, entitled "Third Working Draft (For Discussion and Correction) Legislative Department", was originally leaked, but is now freely available online.[17] The draft supports privacy rights broadly, and includes a strong mechanism to address breaches of the right to privacy, called the Data Protection Authority of India (DPAI). Without privacy laws and safeguards to protect data, the collection and retention of such data can be misused easily, and this could have a chilling effect on free speech among the Indian population. Most Indian members of parliament are aware of the need for a legal framework to protect the privacy of Indian citizens. In 2011, the parliament passed new data protection rules; however, there is still no privacy law in India. Like freedom of expression and freedom of association, privacy is a fundamental human right and underpins human dignity.

A road ahead

The following actions and steps are recommended for India:

- To take better account of the right to privacy and protection from arbitrary interference with privacy. There is also a need to address mass surveillance and unwarranted digital intrusions in India. Both are necessary steps to fight self-censorship and promote freedom of expression.
- Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society.

12 www.indigovision.com/documents/public/project-briefs/Project-Brief-Delhi%20Airport-UK.pdf

13 www.google.com/transparencyreport/userdatarequests/IN

14 Gallagher, R. (2013, February 22). India's spies want data en every BlackBerry customer worldwide. *Slate*. www.slate.com/blogs/future_tense/2013/02/22/india_wants_data_on_every_blackberry_customer_worldwide.html

15 The Constitution of India, Article 19 (2).

16 www.legalserviceindia.com/articles/art222.htm

17 Available at: bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf

- Reform the Information Technology Act provisions 66A and 79 regarding takedown procedures so that authors of content can be notified and offered the opportunity to appeal takedown requests before censorship occurs.
- Revise takedown procedures so that demands for the removal of online content do not apply to the legitimate expression of opinions or content in the public interest. This is important so that freedom of expression is not undermined.
- The internet should not be used by governments as an excuse for introducing new technologies of control or for curtailing existing liberties. Although the right to freedom of expression can be restricted, the circumstances under which this may be done have to be narrowly circumscribed. This is the case when it comes to freedom of expression on the internet, and in any other forum.
- In a country like India where 243 million people access the web through mobile phones, there is a need to reform policy so that regulation of the internet is compatible with the international legal guarantee of the right to freedom of expression. Moreover, there is a need to promote access to the internet as well as the development of local content.
- Service providers or hardware or software vendors should not be compelled to build surveillance or backdoors into their systems, or to collect or retain particular information purely for state surveillance purposes.
- Finally, there are many aspects involving the right to privacy and freedom of expression that relate to each other and that have not been addressed strongly in Indian legislation, policy or case law. For example, the taking of photographs by individuals (not the media) has not been addressed, nor has the ability of individuals to issue comments anonymously online, or the "right to be forgotten" online and offline. Freedom of expression and privacy support each other in many ways, as the right to express an opinion or thought freely is often protected by providing the individual the privacy (or anonymity) to do so. There is therefore a need to understand various aspects, such as the right to be anonymous, the right to privacy, and the right to be forgotten, with respect to freedom of expression and freedom of association. These issues are being addressed by many countries and at an international level.

It is high time the Indian government took account of the right to privacy and protection instead of interfering with privacy. Addressing the issue of mass surveillance and unwarranted digital intrusions is a vital and important step to fight against self-censorship in India and will automatically promote freedom of expression.