THE CENTRE FOR INTERNET AND SOCIETY

PRIVACY AND SURVEILLANCE ROUNDTABLE

JUNE 28TH 2014
MUMBAI, INDIA

ABOUT THE ROUNDTABLES

The Privacy and Surveillance Roundtables are a CIS initiative, in partnership with the Cellular Operators Association of India (COAI), as well as local partners. From June 2014 – November 2014, CIS and COAI will host seven Privacy and Surveillance Roundtable discussions across multiple cities in India. The Roundtables will be closed-door deliberations involving multiple stakeholders. Through the course of these discussions we aim to deliberate upon the current legal framework for surveillance in India, and discuss possible frameworks for surveillance in India. The provisions of the draft CIS Privacy Bill 2013, the International Principles on the Application of Human Rights to Communication Surveillance, and the Report of the Group of Experts on Privacy will be used as background material and entry points into the discussion. The recommendations and dialogue from each roundtable will be compiled and submitted to the Department of Personnel and training

The first of seven proposed roundtable meetings on "Privacy and Surveillance" conducted by the Centre for Internet and Society in collaboration with the Cellular Operators Association of India and the Council for Fair Business Practices was held in Mumbai on the 28th of June, 2014.

The roundtable's discussion centered on the Draft Privacy Protection Bill formed by CIS in 2013, which contains provisions on the regulation of interception and surveillance and its implications on individual privacy. Other background documents to the event included the Report of the Group of Experts on Privacy, and the International Principles on the Application of Human Rights to Communications Surveillance

BACKGROUND AND CONTEXT

The Chair of the Roundtable began by giving a brief background of Surveillance regulation in India, focusing its scope to primarily telegraphic, postal and electronic surveillance.

Why a surveillance regime now?

A move to review the existing privacy laws in India came in the wake of Indo-EU Fair Trade Agreement negotiations; where a Data Adequacy Assessment conducted by European Commission found India's data protection policies and practices inadequate for India to be granted EU secure status. The EU's data protection regime is in contrast, fairly strong, governed by the framework of the EU Data Protection Directive, 1995.

In response to this, the Department of Personnel and Training, which drafted the Right to Information Act of 2005 and the Whistleblower's Protection Act, 2011 was given the task of forming a Privacy Bill. Although the initial draft of the Bill was made available to the public,

as per reports, the Second draft of the Bill has been shared selectively with certain security agencies and not with service providers or the public.

DISCUSSION

The Chair began the discussion by posing certain preliminary questions to the Roundtable:

- What should a surveillance law contain and how should it function?
- If the system is warrant based, who would be competent to execute it?
- Can any government department be allowed a surveillance request?

A larger question posed was whether the concerns and questions posed above would be irrelevant with the possible enforcement of a Central Monitoring System in the near future? As per reports, the Central Monitoring System would allow the government to intercept communications independently without using service providers and thus, in effect, shielding such information from the public entirely.

The CIS Privacy Protection Bill's Regulatory Mechanism

The discussion then focused on the type of regulatory mechanism that a privacy and surveillance regime in India should have in place. The participants did not find favour in either a quasi-judicial body or a self-regulatory system – instead opting for a strict regulatory regime.

The CIS Draft Privacy Protection Bill proposes a regime that consists of a Data Protection Regulation Authority that is similar to the Telecom Regulatory Authority of India, including the provision for an appellate body. The Bill envisions that the Authority will act as an adjudicating body for all complaints relating to the handling of personal data in addition to forming and reviewing rules on personal data protection.

Although, the Draft Bill dealt with privacy and surveillance under one regulatory authority, the Chair proposes a division between the two frameworks, as the former is governed primarily by civil law, and the latter is regulated by criminal law and procedure. Though in a 2014 leaked version of the governments Privacy Bill, surveillance and privacy are addressed under one regulation, as per reports, the Department of Personnel and Training is also considering creating two separate regulations: one for data protection and one for surveillance.

Authorities in Other Jurisdictions

The discussion then moved to comparing the regulatory authorities within other jurisdictions and the procedures followed by them. The focus was largely on the United States and the United Kingdom, which have marked differences in their privacy and surveillance systems.

In the United Kingdom, for example, a surveillance order is reviewed by an Independent Commissioner followed by an Appellate Tribunal, which has the power to award compensation. In contrast, the United States follows a far less transparent system which governs foreigners and citizens under separate legislations. A secret court was set up under the FISA, an independent review process, however, exists for such orders within this framework.

The Authority for Authorizing Surveillance in India

The authority for regulating requests for interceptions of communication under the Draft CIS Privacy Protection Bill is a magistrate. As per the procedure, an authorised officer must approach the Magistrate for approval of a warrant for surveillance. Two participants felt that a Magistrate is not the appropriate authority to regulate surveillance requests as it would mean vesting power in a few people, who are not elected via a democratic process.

In the present regime, the regulation of interception of telecommunications under Indian Law is governed by the Telegraph Act,1885 and the Telegraph Rules,1951. Section 5(2) of the Act and Rule 419A of the Telegraph Rules, permit interception only after an order of approval from the Home Secretary of the Union Government or of the State Governments, which in urgent cases, can be granted by an officer of the Joint Secretary Level or above of the Ministry of Home Affairs of the Union or that State's Government.

Although most participants felt confident that a judicial authority rather than an executive authority would serve as the best platform for regulating surveillance, there was debate on what level of a Magistrate Judge would be apt for receiving and authorizing surveillance requests - or whether the judge should be a Magistrate at all. Certain participants felt that even District Magistrates would not have the competence and knowledge to adjudicate on these matters. The possibility of making High Court Judges the authorities responsible for authorizing surveillance requests was also suggested. To this suggestion participants noted that there are not enough High Court judges for such a system as of now.

The next issue raised was whether the judges of the surveillance system should be independent or not, and if the orders of the Courts are to be kept secret, would this then compromise the independence of such regulators. As part of this discussion, questions were raised about the procedures under the Foreign Intelligence Surveillance Act, the US regulation governing the surveillance of foreign individuals, and if such secrecy could be afforded in India. During the discussions, certain stakeholders felt that a system of surveillance regulation in India should be kept secret in the interests of national security. Others highlighted that this is the existing practice in India giving the example of the Intelligence Bureau and Research and Analysis Wing orders which are completely private, adding however, that none of these surveillance regulations in India have provisions on disclosure.

When can interception of communications take place?

The interception of communications under the CIS Privacy Protection Bill is governed by the submission of a report by an authorised officer to a Magistrate who issues a warrant for such surveillance. Under the relevant provision, the threshold for warranting surveillance is suspicious conduct. Several participants felt that the term 'suspicious conduct' was too wide and discretionary to justify the interception of communication and suggested a far higher threshold for surveillance. Citing the Amar Singh Case, a participant stated that a good way to ensure 'raise the bar' and avoid frivolous interception requests would be to require officers submitting interception request to issue affidavits. A participant suggested that authorising officers could be held responsible for issuing frivolous interception requests. Some participants agreed, but felt that there is a need for a higher and stronger standard for interception before provisions are made for penalising an officer. As part of this discussion, a stakeholder added that the term "person" i.e. the subject of surveillance needed definition within the Bill.

The discussion then moved to comparing other jurisdictions' thresholds on permitting surveillance. The Chair explained here that the US follows the rule of probable cause, which is where a reasonable suspicion exists, coupled with circumstances that could prove such a suspicion true. The UK follows the standard of 'reasonable suspicion', a comparatively lesser degree of strength than probable cause. In India, the standard for telephonic interception under the Telegraph Act 1885 is the "occurrence of any public emergency or in the interest of public safety" on the satisfaction of the Home Secretary/Administrative Officer.

The participants, while rejecting the standard of 'suspicious conduct' and agreeing that a stronger threshold was needed, were unable to offer other possible alternatives.

Multiple warrants, Storing and sharing of Information by Governmental Agencies

The provision for interception in the CIS Privacy Protection Bill stipulates that a request for surveillance should be accompanied by warrants previously issued with respect to that individual. The recovery of prior warrants suggests the sharing of information of surveillance warrants across multiple governmental agencies which certain participants agree, could prevent the duplication of warrants.

Participants briefly discussed how the Central Monitoring System will allow for a permanent log of all surveillance activities to be recorded and stored, and the privacy implications of this. It was noted that as per reports, the hardware purported to be used for interception by the CMS is Israeli, and is designed to store a log of all metadata.

A participant stated that automation component of the Centralized Monitoring System may be positive considering that authentication of requests i.e. tracing the source of the interception may be made easier with such a system.

Conditions prior to issuing warrant

The CIS Privacy Protect Bill states that a Magistrate should be satisfied of either

A reasonable threat to national security, defence or public order; or a cognisable offence, the prevention, investigation or prosecution of which is necessary in the public interest When discussing these standards, certain participants felt that the inclusion of 'cognizable offences' was too broad, whereas others suggested that the offences would necessarily require an interception to be conducted should be listed. This led to further discussion on what kind of categorisation should be followed and whether there would be any requirement for disclosure when the list is narrowed down to graver and serious offences.

The chair also posed the question as to whether the term 'national security' should elaborated upon, highlighting the lack of a definition in spite of two landmark Supreme Court judgments on national security legislations, Terrorist and Disruptive Activities Act,1985 and the Prevention of Terrorism Act, i.e. Kartar Singh v Union of India[1] and PUCL v Union of India[2].

Kinds of information and degree of control

The discussion then focused on the kinds of information that can be intercepted and collected. A crucial distinction was made here, between content data and metadata, the former being the content of the communication itself and the latter being information about the communication. As per Indian law, only content data is regulated and not meta-data. On whether a warrant should be issued by a Magistrate in his chambers or in camera, most participants agreed that in chambers was the better alternative. However, under the CIS Privacy Protection Bill, in chamber proceedings have been made optional, which stakeholders agreed should be discretionary depending on the case and its sensitivity.

Evidentiary Value

The foundation of this discussion, the Chair noted, is the evidentiary value given to information collected from interception of communications. For instance, the United States follows the exclusionary rule, also known as the "fruit of the poisonous tree rule", where evidence collected from an improper investigation discredits the evidence itself as well as further evidence found on the basis of it.

Indian courts however, allow for the admission of evidence collected through improper collection, as does the UK. In *Malkani v State of Maharashtra*[3], the Supreme Court stated that an electronically recorded conversation can be admissible as evidence, and stated that evidence collected from an improper investigation can be relied upon for the discovery of further evidence - thereby negating the application of the exclusionary rule.

Emergent Circumstances: who should the authority be?

The next question posed to the participants was who the apt authority would be to allow surveillance in emergent circumstances. The CIS Privacy Protection Bill places this power with the Home Secretary, stating that if the Home Secretary is satisfied of a grave threat to national security, defence or public order, he can permit surveillance. The existing law under

[1] 1994 4 SCC 569
[2] (1997) 1 SCC 301
[3] [1973] 2 S.C.R. 417

the Telegraph Act 1885 uses the term 'unavoidable circumstance', though not elaborating on what this amounts to for such situations, where an officer not below the rank of a Joint Secretary evaluates the request. In response to this question, a stakeholder suggested that the issuing authority should be limited to the police and administrative services alone. In the CIS Privacy Protection Bill - a review committee for such decisions relating to interception is comprised of senior administrative officials both at the Central and State Government level. A participant suggested that the review committee should also include the Defence secretary and the Home secretary.

Sharing of Information

The CIS Privacy Protection Bill states that information gathered from surveillance should not be shared be shared amongst persons, with the exception that if the information is sensitive in terms of national security or prejudicing an investigation, an authorised officer can share the information with an authorised officer of any other competent organisation.

A participant highlighted that this provision is lacking an authority for determining the sharing of information. Another participant noted that the sharing of information should be limited amongst certain governmental agencies, rather than to 'any competent organisation.'

Proposals for Telecommunication Service Providers

In the Indian interception regime, although surveillance orders are passed by the Government, the actual interception of communication is done by the service provider. Certain proposals have been introduced to protect service providers from liability. For example, an execution provision ensures that a warrant is not served on a service provider more than seven days after it is issued. In addition an indemnity provision prevents any action being taken against a service provider in a court of law, and indemnifies them against any losses that arise from the execution of the warrant, but not outside the scope of the warrant. During discussions, stakeholders felt that the standard should be a blanket indemnity without any conditions to assure service providers.

Under the Indian interception regime, a service provider must also ensure confidentiality of the content and meta data of the intercepted communications. To this, a participant suggested that in situations of information collection, a service provider may have a policy for obtaining customer consent prior to the interception. The Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011 are clearer in this respect, which allow for the disclosure of information to governmental agencies without consent.

Another participant mentioned that the inconsistencies between laws on information disclosure and collection, such as the IT Act, the Right to Information Act and the recently enacted Whistleblower's Protection Act, 2011 need to be harmonised. Other stakeholders agreed with this, though they stated that surveillance regulations should prevail over other laws in case of any inconsistency.

CONCLUSIONS

The inputs from the Bombay Roundtable seem to point towards a more regulated approach, with the addition of a review system to enhance accountability. While most stakeholders here agreed that national security is a criterion that takes precedence over concerns of privacy vis-à-vis surveillance, there is a concomitant need to define the limits of permissible interception. The view here is that a judicial model would prove to be a better system than the executive system; however, there is no clear answer as of yet on who would constitute this model. While the procedure for interception was covered in depth, the nature of the information itself was covered briefly and more discussion would be welcome here in forthcoming sessions.