Centre for Internet and Society (CIS)

Delhi Privacy Round Table Meeting

13th April 2013

Report

In furtherance of Internet Governance multi-stakeholder Initiatives and Dialogue in 2013, the Centre for Internet and Society (CIS) in collaboration with the Federation of Indian Chambers of Commerce and Industry (FICCI), is holding a series of six multi-stakeholder round table meetings on "privacy" from April 2013 to August 2013. DSCI will be joining the CIS as a co-organizer on 20 April 2013. The CIS is undertaking this initiative as part of their work with Privacy International UK on the SAFEGUARD project.

In 2012, the CIS was a member of the Justice AP Shah Committee which created the "Report of Groups of Experts on Privacy". The CIS has recently drafted a Privacy (Protection) Bill 2013, with the objective of contributing to privacy legislation in India. The CIS has also volunteered to champion the session/workshops on "privacy" in the final meeting on Internet Governance proposed for October 2013.

At the roundtables the Report of the Group of Experts on Privacy and the text of the Privacy (Protection) Bill 2013 will be discussed. The discussions and recommendations from the six round table meetings will be presented at the Internet Governance meeting in October 2013.

The dates of the six Privacy Round Table meetings are enlisted below:

1. New Delhi Roundtable: 13 April 2013
2. Bangalore Roundtable: 20 April 2013
3. Chennai Roundtable: 18 May 2013
4. Mumbai Roundtable: 15 June 2013
5. Kolkata Roundtable: 13 July 2013
6. New Delhi Final Roundtable and National Meeting: 17 August 2013

This report entails an overview of the discussions and recommendations of the first Privacy Round Table meeting in New Delhi, on 13th April 2013.

Overview of Justice A P Shah Report: Purpose, Principles and Framework

The meeting began with an overview of the Report of the Group of Experts on Privacy, by the Justice AP Shah Committee. The report recommends a potential framework for privacy in India, including detailing nine privacy principles and a regulatory framework. India currently lacks a privacy legislation and during the meeting it was pointed out that the protection of personal data in India is a highly significant issue, especially in light of the UID scheme. The Report of the Group of Experts on Privacy has guided the draft of the Privacy (Protection) Bill 2013 by CIS and will potentially guide the creation of privacy legislation by the Government of India.

During the discussion on the report, a participant stated that, although a privacy legislation should be enacted in India to protect individuals´ personal data, commercial interests should not be endangered in the name of privacy. In particular, he called upon the need for the creation of a comprehensive privacy law in India and argued that although privacy should be protected, it should not have a negative impact on cloud computing, social media and on online businesses. Thus, the participant emphasized upon the creation of "light-weight" privacy legislation, which would protect individual´s right to privacy, without infringing upon the interests of the private sector.

Following the presentation of the privacy principles of the Justice AP Shah Report, the participants of the meeting made many comments on the feasibility of applying these principles within privacy legislation. In particular, a participant stated that setting a specific data retention framework is a very complicated issue, since the storage of data depends on many factors, some of which are:

- The purpose of the collection of data
- The purpose behind the collection of data may change within the process and may require a longer retention period, depending on the case
- Data is shared with third parties and it is hard to control how long they retain the data for
- Every type of data serves a different purpose and it is hard to set a universal data retention regulatory framework for all different types of data

Some participants argued that the nature of technological evolution should be considered within the privacy principles framework, in the sense that privacy is a fundamental human right to the extent that it does not disrupt other human rights and interests, such as those of companies. Many questions were raised in regards to data collection, one of them being: When data is collected for two different purposes, should an individual be eligible to single access of both types of data? Many other questions were raised in regards to co-regulation and self-regulation. In particular, a participant argued that, based on international

experience, India will not be able to enforce self-regulation. On self-regulation in the United States, a participant stated that there are fifty laws which deal with certain aspects of privacy. The participant suggested that India follows the U.S. model, since self-regulation is more effective when the industry is involved, rather than when the government just imposes laws in a top-down manner. The United States enables the involvement of the industry in self-regulation and a participant recommended the same for India, as well as that the standards for co-regulation and self-regulation are approved by the Privacy Commissioner.

While identifying the clash between the right to privacy and the right to information, participants argued that safeguards are essential in a co-regulation framework, to ensure transparency. It was emphasized that India has a history of corruption and abuse of government power, which increases the probability of self-regulation in the country not being successful. India is currently facing serious problems of accountability and lack of transparency, and participants argued that a solid legal privacy framework would have to be reached, which would not require a legal amendment every other month. Participants pointed out that, within the privacy context, it is highly significant to identify where incentives lie and to regulate the Privacy Commissioner. Currently, if an officer denies access to information, it could take at least a year and a half before being authorised access to information. Participants argued that IT companies and law enforcement agencies should be enabled to access information and that the denial of access to information by the Privacy Commissioner should be regulated. In particular, participants referred to examples from the UK and questioned whether Privacy Commissioners should be considered public authorities.

The need to find a mechanism which would inform individuals of how their data is used was discussed during the meeting. A debate revolved around the question of whether the Indian government should inform an individual, once that individual´s personal information has been collected, used, processed and retained. Many participants argued that since customers decide to use their products, they should comply with the companies´ method of handling data and they should trust that the company will not misuse that data. This argument was countered by other participants, who argued that companies should be accountable as to how they handle customers´ data and that the sharing of customer data without the individual´s prior knowledge or consent could lead to data breaches and human rights violation.

The first hour of the meeting concluded that self-regulation should be considered in regards to IT companies dealing with customers´ data, but a consensus on whether companies should inform individuals of how their data is being used was not reached. Nonetheless, everyone in the meeting agreed upon the need to introduce privacy legislation in India, especially since phone tapping and the interception of communications is a widespread phenomenon in the country. India currently lacks rules for CDRs and the introduction of procedures and laws which would regulate the interception of communications in India was

generally agreed upon throughout the first session of the meeting, even though the technical details of how data would be used by the private sector remained controversial.

Discussion Highlights:

- The pros and cons of self-regulation and co-regulation
- The national privacy principles – and how to build in insurance for technology
- The role of the Privacy Commissioner
- The definition of terms used in the draft Privacy (Protection) Bill 2013

Overview, explanation and discussion on the Privacy (Protection) Bill 2013

The second session of the meeting began with an overview of the Privacy (Protection) Bill 2013, which was drafted by the Centre for Internet and Society (CIS) and represents a citizen´s version of a privacy legislation for India. The Bill entails chapters on the definition of privacy, personal data, interception, surveillance and the Privacy Commissioner. The surveillance chapter was not thoroughly discussed during the meeting, as it is primarily handled from a criminal law perspective and the majority of the participants were from the IT sector.

During the meeting, the possibility of splitting the Bill was discussed. In particular, if separated, one Bill would focus on personal data and interception, while the second would focus on the criminal justice system. This would broadly be along the lines of the Canadian regime, which has two separate legislations to deal with privacy in the private and public sector.

Participants discussed the possibility of narrowing down the scope of the exceptions to the right to privacy, and made the critique that the Bill does not include any provisions for co-regulation and self-regulation. Many participants insisted that self-regulation should be included in the Bill, while other participants pointed out that the Bill does not provide protection for very several types of data, such as sexual orientation, caste and religion, which may be problematic in the future.

As the draft Privacy (Protection) Bill 2013 may possibly clash with pre-existing laws, such as the IT Act, participants recommended that new definitions be created, to ensure that the proposed privacy legislation coincides with other contradicting legislation. Many questions were raised in regards to how personal data in the public sector would be distinguished by personal data in the private sector. Other questions were raised on the harmonization of the Privacy Bill with the Right to Information Act, as well as on the redefinition of surveillance and interception, their changing nature and the difficulties of regulating them.

Many participants agreed that India´s proposed Privacy Law should meet *global standards* in order to attract more customers to Indian IT companies. However, a participant disagreed with this notion and argued that privacy principles generally differ depending on the social, economic, political and cultural status of a country and that the same universal privacy principles should not be imposed upon all countries. The participant argued that India should not copy global standards, but should instead create parallel legislation which would be interoperable with global standards.

The issue of to whom privacy laws would apply to was thoroughly discussed during the meeting. In particular, questions were raised in regards to whether privacy legislation would only apply to Indian individuals, or if it would also apply to international individuals using services and/or products by Indian IT companies. The data protection of customers beyond India remains vague and this was thoroughly discussed, while participants disagreed upon this issue. According to the draft Privacy (Protection) Bill 2013, consent needs to be taken from the individual, but it remains unclear whether that would be applicable to international customers. Questions were raised on how Indian IT companies would gain consent on the use of data by customers of foreign countries, especially since different laws apply to each country.

The second session of the meeting also entailed a debate on the disclosure of data to intelligence agencies by IT companies. Public authorities often request data from IT companies, on the grounds of national security and the prevention of crime and terrorism. However, questions were raised on whether companies should inform the individual prior to disclosing data to public authorities, as well as on whether certain terms, such as ´data´, should be reconceptualised.

The term ´sensitive personal data´ was analysed in the meeting and it was argued that it entails data such as sexual orientation, religion, caste and health records among others. The participants emphasized the significance of the Bill explicitly including the protection of all sensitive personal data, as well as the need to provide requirements for using personal data in both the private and public sphere. Some participants suggested that the Privacy Commissioner in India be empowered with the authority to define the term ´sensitive personal data´ and that he/she not only ensures that all such data is legally protected, but also that health data is included within the definition of the term. A participant backed up the need to closely define the term ´sensitive personal data´, by arguing that a loose definition of the term, which would not include ethnic origin, could lead to social violence and tension and thus the necessity to strictly define the term is highly essential.

Throughout the meeting it was pointed out that the Bill only deals with three aspects of privacy: personal data, surveillance and interception of communications. According to the draft Privacy (Protection) Bill 2013, an individual has the right to install surveillance technology in his/her private property, as long as that technology does not monitor other individuals in private areas. A participant asked about the balance between internet

freedom and privacy, whether that should be included in the Bill and whether exemptions to privacy should be included within those lines. Other participants asked whether CDR records should be placed under privacy exemptions and whether the public disclosure of surveillance should be prohibited by the Bill. The need to redefine ´public figures´ was also emphasized in the meeting, as the threshold for public disclosure of data remains unclear. Some participants argued that the public disclosure of data should be prohibited, as this may potentially have severe effects on vulnerable groups of people, such as victims of violence. However, several participants disagreed by arguing that disclosure of data in the name of public interest should be enabled.

During the meeting several participants argued that the fact that many social networking sites and other online social media enable individuals to publicize their personal data makes it even harder to protect their online privacy. A participant emphasized the need to take freedom of expression into consideration, as it significantly enables individuals to disclose their personal data and increases the probability of online data breaches. Thus, it was argued that the draft Bill should distinguish between private data and private data being made publicly available. However, a participant argued that publicly available data depends on *where* it is being broadcasted. To support this argument, an example was brought forward of an individual uploading a video on YouTube and that same video being broadcasted on national television. Thus the context in which data is made publicly available is highly significant and should be outlined within the draft Privacy Bill.

The meeting proceeded to a discussion on the interception of communications and a participant claimed that a major privacy abuse is to intercept communications without a warrant or a legal order, and to request for authorisation once the interception has already being conducted. It was argued that, in any case, legal authorisation prior to any interception should be a prerequisite and should be highlighted in the draft Privacy Bill. However, another participant argued that currently, the interception of communications needs to be legally authorised within seven days and that prior authorisation should not be a prerequisite. This argument was supported by the statement that in extreme cases, the conditions may not enable prior authorisation. Many participants then questioned this practice by asking what happens in cases when authorisation is not granted within seven days after an interception and whether the agencies conducting the interception would be accountable. An assertive answer was not given, but the majority of the participants appeared to agree upon the need for legal authorisation prior to any interception.

The second session of the meeting concluded to the significance of the principles of notice and consent, which should apply in every case, prior to every interception of communications and in regards to the handling of all individuals´ personal data.

Discussion Highlights:

- If the draft Privacy (Protection) Bill 2013 should be split to two separate Bills
  Definition for the term ´sensitive personal data´ (to include broader categories, such as health data)
- If personal data should be distinguished in the private and public sector
- If the draft Privacy (Protection) Bill 2013 should comply with global privacy standards
- The nuances of consumer consent
- Various ways to define ´public figures´
- Freedom of expression in the context of the draft Privacy (Protection) Bill 2013
- The distinction between exemptions and exceptions

In depth explanation and discussions regarding the Privacy (Protection) Bill 2013

The third and final session of the Privacy Round Table began with a discussion on data collection. In particular, a participant stated that data collection should not be defined for a specific purpose, as the purposes for data collection constantly change. This argument was supported by the statement that privacy provisions can negatively affect a company and reduce its earnings, since restricting the instances for data collection ultimately restricts the services a company can provide (such as advertising). Thus it was strongly argued that data collection should not be restricted to ´specific purposes´, because such purposes can constantly change and all such restrictions can have a negative impact on both the industry and on intelligence agencies carrying out crime investigations. Other participants countered this argument by stating that the term ´necessary information´ is too broad and vague and could create a potential for abuse, which is why data collection should be restricted to specific instances which are legally justified.

The idea that Internet users should be given the right or the option not to be tracked was emphasized during the meeting. It was suggested that the draft Privacy Bill entails provisions which would oblige IT companies and intelligence agencies to inform an individual prior to the tracking of data and to request consent. This argument was supported by the statement that IT companies should protect the interest of the people, especially in terms of data mining and analytics. All such arguments were countered by a participant who stated that the collateral damage surrounding privacy needs to be acknowledged. This statement was supported by the argument that, although it is important to safeguard individuals´ right to privacy, regulations should not infringe upon the rights and interests of companies. In particular, it was argued that a deterrent law should not be created and that it should be acknowledged that individuals *choose* to disclose a large amount of information.

The meeting proceeded to the discussion of the disclosure of data to third parties, and many participants argued that they should not be obliged to disclose the names of the parties they are sharing data with. It was argued that businesses prefer not to reveal the names of the third parties to which they are disclosing data to, as this would affect their competitive advantage in the market. This argument was supplemented by the statement that it would not be feasible to inform individuals every time their data is being shared and that not only would this affect a company´s competitive advantage in the market, but it would also be costly and time consuming. Instead of informing individuals every time their data is being shared, it was argued that companies are responsible for protecting their customers´ data and that those customers should trust companies with their data. A participant strongly argued that while companies are obliged to protect their customers´ data, they are not obliged to reveal the parties with whom they are sharing information with, as this would be highly inconvenient.

Many participants strongly reacted to these statements by arguing that customers should have the right to be informed of how their data is being used and with which parties it is being shared. A participant argued that a customer may not trust the parties that the company chooses to trust and thus every customer should be informed of the sharing of their data. The customer should be respected and should be informed about the sharing of his/her personal data with third parties, because when data is being outsourced, the customer can only hope that the third parties handling his/her data will not misuse it. Thus, customers ultimately lose control over their data and over their personal lives. In order to avoid potential privacy breaches and to empower individuals with control over their personal data and their lives, it was argued that companies should be obliged to inform individuals of the sharing of their data and that this provision should be included in the draft Privacy Bill.

A participant countered this argument by stating that when data is being automated, it is hard to identify the source of the data and that by providing transparency on which parties share customer data, companies would be put out of business. A participant responded to this argument by stating that companies only protect users´ data when they have an incentive to do so, which is why a liability element should be added to the Bill. Other participants supported the argument of not informing customers of the handling of their data by stating that even some of the biggest IT companies, such as Gmail, share customers data with third parties without informing individuals or gaining prior consent. Such arguments were supported by other participants who emphasized upon the futility of informing customers of the handling of their data, especially since the average customer would not understand the security setting of a server. Since the majority of online users lack the technological expertise to understand the security settings, all companies should do is provide a security assurance to their customers in regards to how their data is being used.

In terms of data retention, a participant repeated the argument that a specific regulatory framework for data retention should not be established, especially since the purpose of data collection may change within time. Thus it was emphasized that no data retention period should be included within the draft Privacy Bill.

In terms of transparency, some participants argued that IT companies should submit detailed reports on how they are using customers' data to the Privacy Commissioner, but not to the public. In particular, many participants emphasized that a co-regulation framework should be implemented for the use of data, through which IT companies would regulate the use of data in co-operation with the Privacy Commissioner. Under a co-regulation framework, the public would be excluded from the right to receive detailed reports on how data is being used. Yet, participants emphasized that companies would be in compliance with regulations on data protection and security, which would ensure that customers´ data is not breached.

Such arguments were countered by other participants, who argued that a tremendous amount of significance lies in informing online users of what type of data is being collected, whether it is being analysed and processed, why it is being collected and with which parties it is being shared with. Such questions are considered to be crucial elements of privacy, especially since privacy means that individuals are able to share some data with some individuals, and choose not to share the same or other data with other individuals. The practices of non-disclosure supported by some participants appear to be infringing upon the core of privacy. The participants emphasized that privacy cannot be protected if companies are not accountable in regards to how they handle data.

The fact that companies can use meta-data for research purposes was mentioned in the meeting, which called upon the need to redefine the term ´data´. Questions were raised in regards to how data can be deleted once used within analytics. Some participants referred to the ´Right to be Forgotten´ debate and stated that the deletion of data, in many cases, is not feasible. A participant stated that some data is very sensitive and that companies should be responsible for deciding on how such data should be handled. Data should not be disclosed for the sake of being disclosed, but companies should decide upon the disclosure, retention and destruction of data based on how sensitive its content is. The participant emphasized that customers directly or indirectly give their consent to their data being handled by companies when they use their products and if they do not agree with the security assurances provided by the companies, then they should use a different product or service. However, this argument was countered by several participants who argued that online consumers do not always have an alternative choice and that there is a difference between the bargaining powers of consumers around the world. Some consumers may be socially pressured into using a specific product or service, or may not have an alternative option and the example of Facebook was brought up. Participants argued that given that

consumers do not always have a choice to use or not use a specific online service, their data should be protected regardless of consent.

The debate on the destruction of data continued with participants arguing that companies should not have to destroy all personal data and that such restrictions should only apply to ´sensitive personal data´. The need for the redefinition of the term ´sensitive personal data´ in the draft Privacy Bill was emphasized again, as well as participants´ concern that the purpose behind the collection of data may change within the process and that the regulations which apply in such cases remain vague. In response to issues revolving around the collection of data, a participant recommended the regulation of instances under which data should *not* be used. In terms of consent, several participants argued that it is not rational to expect consumers to give consent for the future (indefinite) use of their data, as this may expose them to future threats which they may have not considered when granting initial consent.

The meeting proceeded to discuss the processing of data and several participants emphasized upon the need to gain consent, whilst others disagreed for the reasons mentioned above. On the disclosure of data, a participant stated that companies can be approached by law enforcement agencies for multiple purposes and that it is usually hard for companies to define the cases under which information is disclosed. Other participants disagreed with the disclosure of data when it is being collected and analysed for investigatory purposes and argued that regulations on the disclosure of data should not be applicable to intelligence agencies.

Discussion Highlights:

- The different instances of data collection and consumer consent
- The nuances of data sharing
- The issue of consumer consent and security assurances offered by companies
- The pros and cons of having a data retention regulatory framework
- How transparency is incorporated into the draft Privacy Protection Bill 2013
- What is needed in provisions that speak to data destruction

Meeting conclusion

The general conclusion of the meeting was that self-regulation should be encouraged, as IT companies should provide security assurances to their consumers and regulate the collection, use, analysis, sharing and retention of their data. There was some discussion on the possibility of introducing co-regulation between IT companies and the Privacy Commissioner, but most participants appeared to prefer self-regulation. All participants in the meeting agreed upon the necessity to introduce a Privacy Bill in India which would safeguard individuals´ right to privacy and other human rights. However, the debate revolved around the definition of terms used in the Bill, whether consent should be a prerequisite to the collection, use, analysis, processing and retention of data, as well as whether companies should be obliged to inform consumers of the sharing, disclosure and destruction of their data.

Following the first Privacy Round Table meeting on the Privacy (Protection) Bill 2013, the discussion between various stakeholders will continue in the next national round table meetings throughout the year 2013.