FRIDAY FEBRUARY 3RD 2012
4:00PM-8:00PM

THE HIGH LEVEL PRIVACY CONCLAVE

PAHARPUR BUSINESS CENTRE, NEHRU PLACE GREENS, NEW DELHI

Conference Report

IDRC CRDI · THE CENTRE FOR INTERNET & SOCIETY · PRIVACY INDIA · PRIVACY INTERNATIONAL · SAG society in action group · CENTRE FOR LAW & POLICY RESEARCH

THE HIGH LEVEL PRIVACY CONCLAVE: A REPORT

Privacy India, the Centre for Internet and Society and the Society in Action Group, with support from IDRC and Privacy International, have spent 18 months studying the state of privacy in India, and conducting consultations across India in Kolkata, Bangalore, Ahmedabad, Guwahati, Chennai, and Mumbai. On February 3, 2012, a high-level conclave was held in New Delhi with representatives from government, industry, media, and civil society participating in the event. At the conclave the discussions were focused on Internet Privacy, National Security & Privacy, and the future of Privacy in India.

Rajan Gandhi, CEO, Society in Action Group, opened the conference with an explanation of the mandate of Privacy India, which is to raise awareness, spark civil action, and promote democratic dialogue around privacy challenges and violations in India. He raised the question of whether Indians are concerned about privacy, while citing examples of banking institutions and telecom service providers, who ask for information more than required, such as marital status, financial status, etc. Lastly, he stressed the need for legislation and awareness about right to privacy.

PANEL I: NATIONAL SECURITY AND PRIVACY

Malavika Jayaram (Advocate, Bangalore) moderated the first panel discussion on "National Security and Privacy". The panel comprised of Manish Tewari (Member of Parliament, Ludhiana), PK Hormis Tharakan (Former Chief of Research and Analysis Wing, Government of India), Gus Hosein (Executive Director, Privacy International, UK), Vakul Sharma (Advocate, Supreme Court), Eric King (Human Rights and Technology Advisor, Privacy International, UK), Amol Sharma (Journalist, Wall Street Journal).

Malavika Jayaram started the discussion by posing the question as to what in their view is 'national security' and when can it be cited by the government to intrude upon our privacy? In response, the panel gave multiple views while agreeing that it is an abstract term. *Gus Hosein*, in response said that national security does not only mean protecting the national border of a nation, but also protecting the rights of the citizen. He also noted that national security is always implemented in a top-down manner. Thus, unfortunately national security has become the stick, which is used to beat down on people's right.

PK Hormis Tharakan defined national security as the security of people and property. National security includes all the efforts of the government to raise poor above the poverty line. He also stated that anything that hinders the process of alleviating poverty is a matter of 'national security'.

Manish Tewari stated that there is a need for legislation to address the various issues of violation of privacy. Specifically, he addressed the need of an independent oversight committee to put a check on the unrestricted powers of the law enforcement and intelligence agencies and the practice of intercepting communications on the grounds of national security. He pointed out that the rules, formulated by the Supreme Court in *PUCL v. Union of India* on interception of communication, are rarely implemented, and the guidelines are implemented more as an exception rather than a rule. The interception of communication by intelligence agencies should be regulated for a larger national interest.

Manish Tewari also observed that there is a nationwide lack of understanding about new technologies and judges are very rarely technologically literate. This has created a situation in which the government's efforts to fight crime and terrorism by intercepting communications has horribly backfired. By building backdoors into communications systems to allow lawful access, and by restricting cryptography to a 40-bit limit, the authorities have created serious vulnerabilities in India's communications system that can be easily exploited by any malicious third party or foreign government.

Privacy Protection

The panel discussion then moved on to the various tools for protecting privacy such data encryption. *Amol Sharma* referred to the process followed in the USA for interception of communication. Surveillance in the United States can be carried out by government agencies only on the basis of a court order or a warrant. He noted that in the US regime there is at least an independent body that gives orders of interception of communication. In comparison, in India, the power to authorize wiretaps lies with the government.

Amol Sharma also pointed out that, there are at least 5000-7000 interception requests from the government, out of which only three to five per cent requests for interception of communication are for white-collar crime. He cited the example of the government asking Research in Motion to provide their encryption keys and also provide a room in their offices for the purpose of interception of communication. He stated that he was very skeptic that terrorists will be using Blackberry services for communication, considering that there are many more convenient and untraceable means available to them such as Skype. He asserted that there is need of legislation for regulation and restricting invasion of privacy. He said, “National security is not a free ticket for any kind of wiretap”.

Concerns about Third Party Intrusion

Eric King noted that national security exists so that individuals can protect themselves from any kind of intrusion. Interception of communication is not only limited to government, equipment for interception of mobile phone calls are easily available and also affordable. So any individual can intercept calls. The notion that interception is only limited to the state is not true, it can be carried out by individuals as well. Heavily criticizing the restriction on encryption in India, he said that the people should be given the power to protect their own privacy. He also harped on the possibility that not only citizens are at risk also government high officials and military personnel can be targeted due to the low level of encryption.

Contributing to the conversation, *Manish Tewari* pointed out that while trying to intercept the mobile phone calls of an individual, the State could listen in to anyone's conversation within the vicinity; hence there are gross privacy violations.

Gus Hosein added that the problem lies at a more basic level. Governments generally order telecom companies to build back door for the purposes of interception. These vulnerabilities in the system are not only used by the government, but also may be misused by third parties. He cited an incident in Greece, where the government asked a telecom service provider to build backdoors into the system. A third party was able to access the back door, during the Athens Olympics, when security was of utmost importance. He also said, "If you build a system that allows the state to listen in to communications, you build national security vulnerability".

This was followed by a Question & Answer session. The issues raised during the Q&A session were:

- Nature of consent given by the user to the telecom service provider. Taking into consideration that service providers have a duty to disclose the user data to the government on request. A situation which gives rise to a binary choice, either use the services or do not use it at all.
- At the wake of breaches in cyber-security, the use of general consumer e-mails by high government officials causes serious threat to nation's security.
- Lack of technical know-how among the government officials.
- If government is inept in handling technology, then are there any concerns about public private partnership and outsourcing of governmental duties. (For example, UID).
- Collection and collation of information by organizations such as NATGRID. Are they vulnerable to misuse?

In the concluding statement of the first panel discussion, Gus Hosein, made the argument that there cannot be a balance between right to privacy and national security, as the former is an individual right and the latter a community right. Community interest will always take precedence over individual right. National security is always the excuse given by government for invading individual privacy.

PANEL II: INTERNET AND PRIVACY

Sunil Abraham (Executive Director, The Centre for Internet and Society, Bangalore) moderated the second panel discussion on “Internet and Privacy”. The panel comprised of Deepak Maheshwari (Director, Corporate Affairs, Microsoft), Amitabh Das (General Counsel, Yahoo! India), Ramanjit Singh Chima (Sr. Policy Analyst, Google), Talish Ray (Board Member, Software Freedom Law Center), and Vinayak Godse (Director- Data Protection, DSCI).

Defining Privacy

Sunil Abraham asked the panel questions with respect to defining privacy in the context of physical privacy and spatial privacy. In response, Amitabh Das said that the right to privacy of individuals should be protected in a similar fashion online, as it is protected offline. Referring to safeguards under *PUCL v. Union of India* (SC, 1996), he observed that communication and behavior on the Internet should be free from monitoring and interception. The procedural safeguards offline should be also present online.

Key Escrow Regime

Deepak Maheshwari talked about the inconsistencies in the encryption standards in India. For example, in case of ISP licensees, there is a 40-bit restriction (symmetric key). In case of adopting higher-level encryption, the ISP has to take permission from the government and deposit both the keys to the government.

He also pointed that online railway ticket booking services use 128-bit encryption. RBI mandates 128-bit encryption for online banking transaction. SBI recommends 64-128 bit encryption. The multiple regulations make it impossible to abide by the rules.

Anonymity and Pseudonymity

Sunil Abraham, while setting the context to India, where the government has taken stringent measures to cut down on anonymity and pseudonymity, asked the question whether such a step is welcomed by the internet users as well as intermediaries. Ramanjit Singh Chima, in reply said that for any business, it is necessary to give what the user wants. Real identity provides a better platform for discussion. He also discussed the choices provided by Google, mainly search without login, encrypted searches so it gives the user to be anonymous. He also noted that there are legal as well as technical restraints as to anonymity on the Internet. He also cited the example of Korea, where the government mandated real name verification process for posting comments on the Internet. Google was not able to comply with this request and had to disable comment section in Korea.

Data Privacy

Vinayak Godse analyzed the issue of data privacy in detail. He stressed upon the need of data privacy law in the country for the outsourcing industries. The European Union (EU) data protection laws govern most of the clients of firms that outsource. EU considers India is not a data safe country due to lack of data privacy legislation. He suggested that the data privacy law should be pragmatic, light touch and should allow industry self-regulation.

Conclusion

The High Level Privacy Conclave discussed various issues related to Internet and privacy and national security and privacy. The various concerns raised by the stakeholders were helpful in understanding the problems related to privacy. The main concerns raised by the first panel were about the interaction and relation of national security to privacy. The major concerns around national security and privacy were of data encryption vis-à-vis surveillance by the State and third party intrusion. There was also an attempt made to understand and define national security in the context of its ambit and when can it be used by the State to access private information. The second panel discussed various aspects of privacy on the Internet. The panel included discussions on anonymity and data privacy on the Internet.

We thank the moderators, panelists and participants for making High Level Privacy a constructive and a fruitful session on privacy and it also gave us insight to understand the problems related privacy and a way forward for possible solutions.