Does India need a separate data protection law?

(Published in the World Data Protection Report Volume 5 Number 12, December 2005)

(By Latha R Nair, Senior Associate, K&S Partners, New Delhi. K&S Partners is a full service Intellectual Property law firm with offices in New Delhi and Bangalore and has a wide ranging practice of IP and IT laws. The author may be contacted at latha@knspartners.com or at +91-11-2955-1801)

India – The Emerging IT super power

In the recent years India has emerged as one of the preferred destinations for offshore business outsourcing. Financial services, educational services, legal services, banking services, healthcare services, marketing services and telecommunication services are just some of the services that are outsourced from India. The factors that have turned India into one of the hotspots for offshore outsourcing are the educated and unemployed masses, enterprising nature of Indians who have excellent spoken English skills and relatively cheap labour. Popularly called BPOs – acronym for Business Process Outsourcing – this industry is multiplying by the day in India.

In June this year, one such BPO was in the eye of the storm when one of its employees sold personal data belonging to a large number of British nationals to an undercover reporter from the British tabloid 'The Sun'. The incident sparked off a debate among the offshore industry circles, media and the legal world as to how safe foreign data is in Indian hands. The discussions were also veered towards the need for some kind of protection for personal data in India which is absent currently.

Proposed Amendments to the Indian Information Technology Act, 2000 – Barking up the wrong tree?

The Ministry of Information Technology also decided to react in its own style and on August 29, 2005, proposed certain amendments to the Information Technology Act, 2000 ("IT Act" for short) and issued a press release in connection therewith[1]. In short, the press release by the Ministry emphasised the need for data protection in the context of BPO operations due to certain "recent developments nationally and internationally". Though not elaborated in the Press Release, the "recent developments" could be a reference to certain incidents including: (i) the sting operation carried out by the Sun on the Indian BPO mentioned before; (ii) the circulation of a multi-media clip depicting the naked body of a woman allegedly morphed with the face of an upcoming Indian actress; (iii) the attempted credit card frauds by an Indian BPO; and (iv) the alleged sale of a sexually explicit multi-media clip depicting a sexual act by two school children (and shot by one of them), on an auction portal owned by e-Bay Inc.

[1] See a copy of the Press Release, Summary of the proposed amendments and Full Text of the report of the Expert Committee at http://www.mit.gov.in/itact2000/index.asp (Visited in November 2005)

Undoubtedly, 2004-2005 has been a tumultuous and eventful year for India's information technology industry. The events described above sent disconcerting ripples of moral outrage through the national conscience, propelling the government to bring out certain amendments to the IT Act to accommodate the concerns being raised. But it looks like the Indian government has got it all jumbled up on the legal front. For better data protection, why should one amend the IT Act, which is meant to be a law to facilitate e-commerce? Aren't e-commerce and data protection two different concepts?

The objective of this article is to look at why India should go for a separate legislation for data protection. In doing so, first, the scope of protection offered by the European Directive on E-commerce and the European Data Protection Directive are examined and distinguished and then the article proceeds to explain why it is inappropriate for India to accommodate data protection provisions into a legislation meant for facilitating e-commerce transactions by specifically examining the recently proposed amendments to the IT Act.

Ecommerce and data protection in Europe –How are they different?

European technology laws have always been in the forefront for moving along with the times. The member countries of the European Union are to legislate national laws for various areas including that of data protection and e-commerce. Some of the European countries have these laws dating back even to the 1970s[2].

As part of the harmonization of the European Union, there are various directives that Member countries are to adopt into their national laws. Two such directives in the areas of data protection and e-commerce are European Directive 95/46/EC ("Data Protection Directive" for short) and European Directive 2000/31/EC ("E-commerce Directive" for short). The Data Protection Directive was enacted for the protection of individuals with regard to the processing of personal data and on the free movement of such data, whereas the E-commerce Directive was enacted with a view to, inter alia, contribute to the proper functioning of the internal market by ensuring free movement of information society services among the member states. It would be useful to examine the scope and reach of both these Directives to understand what is envisaged by each of these.

The Data Protection Directive was enacted in 1995 with the twin objectives of protection of personal data and facilitating the free movement of such data[3]. The said objectives certainly contradict each other and therefore, the Directive seeks to balance these two contradictory objectives. Personal data is defined under the Directive as any information relating to an identified or identifiable natural person. The Directive is to apply to the processing of personal data wholly or partly by automatic means and to the processing otherwise than by automatic means of personal data which forms part of a filing system. Certain types of processing such as processing of personal data for public security, defence, state security and activities in the areas of criminal law and processing by a person in the course of personal or household activities are exempt from the scope of the Directive.

---

[2] French Act No. 78-17 of 6 January 1978 on Data Processing Data Files and Individual Liberties

[3] See Article 1 Object of the Directive 95/46/EC

Under the Directive, member states are under obligation to do the following:

- To ensure that data is processed fairly and lawfully and that it is collected for specified and legitimate purposes and not processed in a manner incompatible with those purposes
- The processing of data is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed
- The data collected is accurate and kept up to date and kept in a form which permits identification of data subjects.
- Personal data may be processed only if
    - the data subject has unambiguously given his consent;
    - processing is necessary for the performance of a contract to which the data subject is party;
    - processing is necessary for compliance with a legal obligation;
    - processing is necessary in order to protect the interests of the data subject;
    - processing is necessary for the performance of a task carried out in the public interest etc.

- The Directive prohibits the processing of certain personal data such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health or sex life or processing for the purposes of preventive medicine, medical diagnosis, offences and criminal convictions etc except under certain conditions.
- To provide to the data subject certain information such as identity of the entity processing the data, purposes of the processing, recipients of the data etc.
- If the data was not obtained from the data subject, member states are to provide that the entity processing the data must provide the data subject with information such as identity of the entity, purposes of processing, categories and recipients of data etc.
- To provide the right to access the data to the data subjects without constraint at reasonable intervals.
- The data subject must be provided a right to object to the processing of data relating to him and where there is a justified objection, it must be provided that the processing may no longer involve the data.
- Apart from imposing an obligation to keep the confidentiality of processing of data, the entity processing the data must be required to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorised disclosure etc.
- The transfer of personal data to third countries by member states must be done only under certain conditions.

The Data Protection Directive, therefore, covers a whole range of issues associated with processing of personal data in keeping with the twin objectives of the Directive.

The E-commerce Directive specifically excludes from its purview issues relating to information society services already covered by the Data Protection Directive[4]. Since its objective is to provide for certain legal aspects of information society services, in particular electronic commerce, the E-commerce Directive stipulates various requirements to be imposed on service providers by member states and required to be complied with by service providers.

To elaborate, the Directive requires a member state to ensure the following:

- That service providers render information such as their name and geographic address, details such as their electronic mail address that allows them to be contacted and communicated with in a direct and effective manner, details of any public registration or identification number etc.
- That commercial communications which are part of an information society service comply with certain conditions such as the communication as well as the person making the communication shall be clearly identifiable etc.
- That unsolicited commercial communication by electronic mail by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient.
- That service providers undertaking unsolicited commercial communications by electronic mail regularly consult the opt-out registers in which persons not wishing to receive such commercial communications can register themselves.
- As regards the treatment of contracts, member states are to ensure that their legal system allows contracts to be concluded by electronic means.
- The Directive also exempts the intermediary service providers of liability in situations when they are mere conduits, in cases of caching and hosting and also stipulates that member states are not to impose a general obligation to monitor on service providers.

Hence, the E-commerce Directive covers issues raised in the context of information society services, the service providers and the obligations of member states regarding such services and the providers of such services.

An overview of both these directives reveal that while the E-commerce Directive deals with all aspects of information society services in detail, the Data Protection Directive deals in detail with one aspect of information society services. Also, while both these directives deal with aspects of information society services, yet the object and concept of both are distinct and different.

Can the proposed amendments to the IT Act, 2000 take care of data protection?

During August this year, the Ministry of Information Technology put up on its website certain proposed amendments to the I T Act, 2000. As mentioned before, the amendments were in the wake of certain recent incidents that took place in India leading to discussions on the growing concerns for the safety of data in India and the need for a data protection law. The following is a list of some of the main proposed amendments as obtained from the website of the Ministry:

[4] See Article 1(5) (b) of Directive 2000/31/EC

- The Act has been made technology neutral by replacing the term 'digital' with 'electronic';
- Section 43 of the Act has been amended to include a new subsection (2) wherein there is a proposal to handle sensitive personal information with reasonable security practices and procedures;
- Section 66 of the Act dealing with computer related offences has been revised to be in line with Section 43 related to penalty for damage to computer resource.
- A new section on Section 67 (2) has been added to address child pornography with higher punishment.
- Keeping in line with the principles in EC Directive 2000/31/EC, section 79 has been revised to bring-out explicitly the extent of liability of intermediary in certain cases.

Hence, the proposed amendments, more of a knee-jerk reaction from the Government to the recent data thefts and other incidents, have more to do with issues related to cyber crimes and e-commerce transactions than data protection. The provisions purportedly for 'data protection' jut out as an ugly patch work on the IT Act and do not offer any comprehensive protection to personal data in India.

Being a major IT power in the global map today, can India afford to deal with an important issue such as this in the manner in which it has dealt with in the proposed amendments to the IT Act? The Indian BPOs and their foreign affiliates are not the only ones bearing the brunt of the lack of a law on data protection. In fact, India is faced with a new phenomenon called telemarketing which has invaded millions of hapless Indians thanks to the widespread use of mobile phones and multiplicity of mobile telephone service providers in India. The tranquillity and comfort of an individual's home or the peaceful conduct of business in an organization is rudely and unabashedly interrupted by telephone calls made by telemarketing executives (who, according to reports, are available for as low as USD 70 per month) on behalf of banks, financial institutions, mobile phone companies etc., with offers of low-interest loans, free credit cards, overdraft facility and the like. Clearly, there is a violation of personal privacy caused by such calls. Unfortunately, India has no statute on privacy laws except for certain provisions of the Constitution of India which have been interpreted by the courts to the effect that the right to privacy is enshrined in the provisions of the Constitution[5].

Besides invading their privacy, such calls also have great potential for annoyance to the recipients since oftentimes they are offered what they do not ever want or what they already have. If the recipient is out of the local area of the service provider, she will have the additional liability of paying roaming charges for such unsolicited calls. Recently, one such annoyed recipient filed a public interest writ petition before the Supreme Court against several banks and mobile phone service providers alleging, *inter alia*, that the respondents are in violation of the

[5] See Mr. X v. Hospital Z (1998) 8 SCC 296 where the court pointed out that the right to privacy is enshrined in Article 21 of the Constitution of India

petitioner's privacy[6]. Notice has been issued to the respondents by the Supreme Court and the matter is coming up before the court again in March 2006. Till such time the writ is decided, the calls will continue unabated.

Without a law in place to curb such intrusive acts, one gets an unnerving feeling of being pried upon because she accidentally gave away valuable private information while filling in a bank account application or mobile phone subscription form! And with a population of over a billion, carelessly provided personal data can be turned into a fortune by telemarketing companies. Hence, there are more reasons than one for the Indian Government to consider enacting a separate data protection law along the lines of Directive 95/46/EC so that the country is in the forefront of legal developments around the world. If India can do it vis-à-vis software, why not law?

[6] A copy of the writ is available at the link http://www.manupatra.com/downloads/2005-data/TelePIL.pdf (last visited in November 2005)