ARRAY Logo

icon

Data Protection in Consumer E-banking*:

Journal of Internet Banking and Commerce, April 2006, vol. 11, no.1
(http://www.arraydev.com/commerce/jibc/)

By Ankur Gupta, Final Year Student/National Law Institute University, Bhopal, India.

Web: www.nliu.com
Email: ankur.gup@gmail.com

Ankur Gupta is a final Year student of law at NLU, Bhopal. His area of interest includes Information Techonology Law, and IPR. He has had publications in these areas in leading Indian newspapers and legal magazines.

Abstract

Consumer Internet Banking, with it's ability to reach each and every nook and cranny of the world holds great importance for a nation like India, where conventional Banking services are out of reach for a large proportion of the masses. But to make it a success it requires more than just an adequate internet enabling infrastructure. There is a dire need for an adequate legal and regulatory framework to be put into place. One of the crucial elements of such a legal and regulatory framework will be Data Protection provisions. The emphasis of this article is on the this aspect of data protection in the electronic banking sector. The article is an attempt to highlight the importance of data protection in internet banking and dwell upon possible legal recourses which may adopted keeping in mind the current legal framework in India with regards regulation of Information Technology.

Law cannot possibly be expected to keep pace with changes in technology. The recent debacle of virtual voyeurism has brought out, amongst other things, the inadequacy and vulnerability of the laws governing use of internet. Fixing liability, recording and reproducing evidence, ascertaining jurisdiction are problems which show little sign of easing. Concerns over security and misuse pertaining to e-banking activity have been mounting as more banks in India foray into electronic banking.

E-banking activities involve not just banks and their customer, but numerous third parties too. Information held by banks about their customers', their transactions etc changes hands several times. It is impossible for banks to retaining information solely within their own computer networks, let alone a single jurisdiction is impossible. Risks pertaining leakage, tampering or blocking of data are sufficiently high to warrant adequate legal and technical protection. India has no law on data protection leave alone a law governing an area as specific as protection of data in electronic banking. Information security in e-banking presents two main areas of risk: preventing unauthorized transactions and maintaining integrity of customers transactions. Data protection falls in the latter category.

Data protection laws primarily aim to safeguard the interest of the individual whose data is handled and processed by others. 'Interests' are usually expressed in terms of privacy, autonomy and/or integrity. Data protection laws are 'framework laws' providing rather diffused general rules for such processing and making allowances for developing detailed norms as and when the need arises. Such legislation typically regulates all or most stages of the data protection cycle including registration, storage, retrieval, and dissemination of personal data. Data protection legislation of a large number of countries, such as Austria, Ireland, Japan, Luxembourg, Sweden and the UK cover only automated data processing practices.

The Indian Information Technology Act, 2000, basically a framework law, makes hacking a punishable offence under Section 66. Breach of information security is implicitly recognized as a penal offence in the form **hacking**. The 'appropriate government' (central/state) is empowered to declare any 'computer', 'computer system' or 'computer network' as a protected system. A ten year prison term and a hefty fine await any person who secures access to the 'secured computer system' in contravention of the provisions of the law.

Despite the deterrence characterized by the penal provisions of the IT Act, 2000, a lacuna in the law is that organizations and entities can take action against those who breach data security procedure, but they are not obliged to implement data security measures to protect consumers and clients. The IT Act does not lay down any such duty upon banks. Contrastingly, in UK, failure to undertake identification of new customers properly can create an array of risks for the bank. Under the Data Protection Act, 1998 an erring bank may face an action for damages if it fails to "maintain adequate security precautions in respect of the data". Essentially, a legal duty is thrust upon the banks, to use reasonable care and skill in disseminating information to persons who access the bank's networks either on the internet or though an ATM card.

In India, a Bank's liability would arise out of contract as there is no statute to the point. When liability is contractual it means that the bank is, by virtue of the contract, under an obligation to keep customers' data secret. If transactions are being done on an open network such as the internet then in case of a security breach, an internet service provider (ISP) may be liable, in addition to the bank. Though ambiguity persists as regards liability of an internet service provider due to dearth of decided case law on the point.

The viability of a sectoral legislation on data protection in e-banking should be gauged. India can take cue from nations which have favored *ad hoc* enactment of sectoral laws over omnibus legislation.

---

* Ankur Gupta, Fourth Year BALLB (hons), National Law Institute University, Bhopal.