1. There is no comprehensive legislation on privacy in India. Explain the problems and challenges faced by Indian Judiciary in handling data privacy issues?

Ans: Internet privacy encompasses a wide range of issues and topics. It can be understood as privacy rights that an individual has online with respect to their data, and violations of the same that take place online. Given the dynamic nature of the online sphere, privacy concerns and issues are rapidly changing. For example – the way in which the internet allows data to be produced, collected, combined, shared, stored, and analyzed is constantly changing and re-defining personal data and what type of protections personal data deserves and can be given. For example, seemingly harmless data such as IP address, key words used in searches, websites visited, can now be combined and analysed to identify individuals and learn personal information about an individual. From information shared on social media sites, to cookies collecting user browser history, to individuals transacting online, to mobile phones registering location data – information about an individual is generated through each use of the internet. In some cases the individual is aware that they are generating information and that it is being collected, but in many cases, the individual is unaware of the information trail that they are leaving online, do not know who is accessing the information, and do not have control over how their information is being handled, and for what purposes it is being used. For example, law enforcement routinely troll social media sites for information that might be useful in an investigation.

The above example also highlights how the “sphere” of information on the internet is unclear i.e. is information posted on social media public information – free for use by any individual or entity including law enforcement, employees, data mining companies etc. or is information posted on social media – private, and thus requires authorization for further use. For example, in India, in 2013 the Mumbai police established a “social media lab” for the purposes of monitoring and tracking user behavior and activities. Authorization is not required for the lab to monitor individuals and their behavior, and individuals are not made aware of the same, as the project claims to analyze only publicly available information. Similar dilemmas have been dealt with by other countries. For example, in the U.S, individuals have contested the use of their tweets without permission, while courts in the US have ruled that tweets, private and public, can be obtained by law enforcement with only a subpoena, as technically the information has been shared with another entity, and is therefore no longer private. Indian Courts have yet to deal directly with the question of social media content being public or private information.

The Complication of Jurisdiction

The borderless nature of information flows over the Internet complicates online privacy, as individual’s data is subjected to different levels of protection depending on which jurisdiction it is residing in. Thus, for example an Indian using Gmail, will be subject to the laws of the United States. On one hand this could be seen as a positive, if one country has stronger privacy protections than another, but could also be damaging to privacy in the reverse situation – where one company has lower privacy standards and safeguards. In addition to the dilemma of different levels of protection being provided over data as it flows through different jurisdictions, access by law enforcement to data stored in a different jurisdiction, or data from one country accessible to law enforcement because it is being processed in their jurisdiction, are two other complications that arise. These complications cannot be emphasized more than with the case of the NSA Leaks. Because Indian data was residing in US servers, the US government could access and use the data with no obligation to the individual. In response to the NSA leaks, the government of India has stated that all facts need to be known before any action is taken, while citizens initially sought to hold the companies who disclosed the data to US security agencies such as Google, Facebook etc. accountable.

Current Policy for Internet Privacy in India

Currently, India’s most comprehensive legal provisions that speak to privacy on the internet can be found in the Information Technology Act (ITA) 2000. The ITA contains a number of provisions that can, in some cases, safeguard online privacy, or in other cases, dilute online privacy. Provisions that clearly protect user privacy include: penalizing child pornography,8 penalizing hacking and fraud9 and defining data protection standards for body corporate.

Provisions that serve to dilute user privacy speak to access by law enforcement to user’s personal information stored by body corporate collection and monitoring of internet traffic data[12] and real time monitoring, interception, and decryption of online communications. Additionally, legislative gaps in the ITA serve to weaken the privacy of online users. For example, the ITA does not address questions and circumstances like the evidentiary status of social media content in India, merging and sharing of data across databases, whether individuals can transmit images of their own “private areas” across the internet, if users have the right to be notified of the presence of cookies and do not track options, the use of electronic personal identifiers across databases, and if individuals have the right to request service providers to take down and delete their personal content.

Online Data Protection

Since 2010, there has been an increasing recognition by both the government and the public that India needs privacy legislation, specifically one that addresses the collection, processing, and use of personal data. The push for adequate data protection standards in India has come both from industry and industrial bodies like DSCI – who regard strong data protection standards as an integral part of business, and from the public, who has voiced increasing concerns that governmental projects, such as the UID, involved with collecting, processing, and using personal data are presently not adequately regulated and are collecting and processing data in such a way that abuses individual privacy. As mentioned above, India’s most comprehensive data protection standards are found in the ITA and are known as the Information Technology “Reasonable security practices and procedures and sensitive personal data or information” Rules 2011.

Cyber Cafés

In 2011 the Guidelines for Cyber Café Rules were notified under the Information Technology Act. These Rules, among other things, require Cyber Cafe’s to retain the following details for every user for a period of one year: details of identification, name, address, contact number, gender, date, computer terminal identification, log in time, and log out time. These details must be submitted to the same agency as directed, on a monthly basis. Cyber Cafes must also retain the history of websites accessed and logs of proxy servers installed at the cyber café for a period of one year. Furthermore, Cyber Café’s must ensure that the partitions between cubicles do not exceed four and half feet in height from floor level. Lastly, the cyber café owner is required to provide every related document, register, and information to any officer authorized by the registration agency on demand. In effect, the identification and retention requirements of these rules both impact privacy and freedom of expression, as cyber cafés users cannot use the facility anonymously and all their information, including browser history, is stored on an a-priori basis. The disclosure provisions in these rules also impact privacy and demonstrate a dilution of access standards for law enforcement to users internet communications as the provision does not define:

- An authorization process by which the registration agency follows to authorize individuals to conduct inspections.