# Privacyand Data Security – a National Need

Lalit Chandak
Span Technologies, New Delhi
lalit@spantel.in

On 24th August, 2017, Supreme Court added a new dimension to the Indian Constitution by ruling that privacy of the individual is now a part of fundamental right to life and personal liberty guaranteed under its Article 21. An individual is now provided with a protective shell in the form of a constitutional cover which provides him with immunity against legislative annulment of his personal liberties.

Such right to privacy existed with liberty and dignity of the individual as found in following Articles of the Indian Constitution when read along with its Preamble:

- *Article 14:* Guaranteeing equal treatment of all citizens.
- *Article 19* (1) (a): Right to free speech and (b) right to assemble without arms.
- *Article 20*: Protection in case of conviction for offenses against the law.
- *Article 21*: Right to life and liberty – specifically, privacy has now been made a part of it.
- *Article 22*: Protection against arrest and detention wthout being informed of grounds.
- *Article 25*: Subject to morality, public order, health and other fundamental rights.

But till the Supreme Court did not define it as a fundamental right, privacy was open to different interpretations viz. in Whatsapp case, Indian Government said that right to privacy is an integral part of Article 21, but in case of Aadhaar, the Government took the opposite view and argued that privacy is not constitutionally inherent. It needs to be understood by all that constitutionally guaranteed right to personal liberty will always stand severely compromised without right to privacy.

While specifically declaring privacy as a fundamental right, it is to be noted that it is not an absolute right. It now restrains the Indian Government from framing any law or policy that in any way impinges on a citizen's right to privacy (as was done when Aadhaar was first introduced for all persons residing in India without any parliamentary approval). Government continues to be allowed to place reasonable restrictions on limited grounds such as national security and public order as allowed in Article 19 (2) with accountability for its actions.

In a rapidly growing digital age, such a situation throws up many aspects of information privacy which now need to be urgently defined by a Data Protection Law in a manner such that while legislation meets privacy needs of the citizen, it does not throttle innovation and economic growth. Rob Sherman, Deputy Chief Privacy officer of Facebook has rightly said that "the best privacy laws across the world are the ones that are based on broad principles and give people the choice to decide what they want to share and with whom".

Different privacy policies will need to be defined in a manner such that it suits a particular situation. Thus what is suitable for social networks will have to be different from what will be required for financial transactions. A fixed set of regulations for privacy will not work. Only such a flexible approach will promote innovation and bring consequent economic benefits.

Increasing digitization is leading to availability of a large number of Government services. We rank among top three adapters of digital technologies and social media. With Government's push for digital payments and GST roll-out, we already account for 2% of daily global transactions. This is expected to grow to 10% in the next 3 to 5 years.

**The Dilemma:**

In order to avail any service on the Internet from any technology company, individuals provide their consent where data generated by their usage when processed becomes the asset of the company. Such data is then used by the company to improve their offering or earn revenue through sales and promotion – not restricted by national boundaries. In order to protect the user's privacy, such data necessarily needs to be anonymised in a manner such that the consumer is not identified by any recipient of such data.

Data so gathered when processed, creates various kinds of data which is proprietary to the company. Such data as a commodity is used for building various new applications and services based on e.g. machine learning and artificial intelligence.

While the user demands privacy, technology companies which are working in a borderless worldand using such data, want light-touch regulations which does not kill innovative usage of such gathered data for building their businesses globally.

Computer resources, IT networks along with all the fixed and mobile devices connected to the Internet comprises borderless cyberspace – all generating big data. Unlike geographical definition in the physical world, cyberspace of a country is limitless with cloud-based flow of data across geographies.

Since India is starting its journey towards big data usage, the government needs to frame regulations which do not hinder future innovation in such a dynamically evolving environment which is not geography bound.

Despite a woefully inadequate WiFi infrastructure, there is a fast growing user interaction over the entire digital eco-system through use of telecom, internet services, apps and devices. All this is generating a large amount of data which is being collected, stored and processed using data analytics. Individuals who have generated such data and have ownership over it are concerned about its privacy, confidentiality and security. Such trust issues arising out of concerns on privacy are thus relevant to services provided by TSPs, ASPs, device manufacturers, operating systems, browsers etc. which collect and process personal data – irrespective of their being in public or private sector. Data integrity has to be at the core of all such consumer offerings.

In these circumstances, let us review some existing systems/operations in India that need a careful relook to be "privacy compliant":

**Aadhaar:**

With Government of India aggressively promoting the use of Aadhaar and its associated ecosystem as a basis of identification and authentication, it needs to be now tested for compliance with defined privacy requirements. The Supreme Court has still to announce their judgement on reasonableness of data collection being done by Aadhaar and if it can be made mandatory for a host of services that the Government is pushing for through coercion and compulsion.

At present, Aadhaar is not a permission based system with the freedom being available to the user to opt-in/opt-out – not only from unique identification database (UID) but also from any of the services linked to it. It is working in a "polysemic model" with UPI and other innovations catering to multiple needs viz. authentication, financial compliances, money transfers, etc. It does not give the user any right to control the use of his digital ID.

For Aadhaar to be privacy compliant, it must **intimate** the user when any of his personal information is sought, purpose of its collection and usage and it will be shared with any third parties. Thereafter,

the user should have the **choice** to opt-in/opt-out. When such permission is given, it should be defined by **limitation** for the purpose it is sought.

In addition to above, the user should have **access** to his Aadhaar data for correction for which Aadhaar should be **open** to providing access in simple language that the user understands while at the same time ensure full **security** against unauthorised access, usage, destruction or hacking. Aadhaar's management needs to be made **accountable** to an independent, autonomous auditing authority (more on it stated later) for ensuring compliance with privacy requirements as per law which investigates breaches of privacy based on complaints by users.

Since Aadhaar is becoming a critical requirement for availing various services in India, it is important to gear it for **multi-factor authentication** in a manner such that it addresses three main factors which combined in different combinations for the basis of authentication: something you are (based on biometric), something you have (based on voter ID/driving license) and something you know (based on pattern, pin or password).

For complete privacy protection, Aadhaar has also to undertake measures where the single ID defined by it for each user - when used to access multiple services – does not provide such common number to any one for matching the records of such user across different databases.

While Justice B.N. Srikrishna Committee is working on a framework and legislation on personal data protection, it needs to look at all the aspects that the new ruling of privacy has generated.

**Browsers, Web-hosted apps and OTT services:**

Access to Internet based websites using browsers, apps and OTT services has made national boundaries irrelevant. In such circumstances, non-state actors also collect and share personal data with third parties across borders with no care or concern about national laws of privacy.In the process of downloading and installing various apps on their phones, users sign away their consent for sharing not only their data but also their contacts data, viz. in case of TrueCaller. At present, India does not have any legal requirement for safeguarding such data. Resolving the issue of individual privacy and data security in such a connected world is also of utmost importance for a nation. This can only happen if hosting servers of some such services that are most widely in use are located within national boundaries.

Thus, the likes of Google, Skype, Facebook, WhatsApp, Twitter etc. have to be told to locate their servers in India. This will result in twin benefits: government will be able to monitor such services for compliance to Indian laws. Additionally, most net traffic to such popular sites will work within national boundaries instead of incurring cost over international pipes. NIXI can play a very important role towards aggregating such national traffic.

**Government service providers, TSPs, ISPs and banks:**

Current authentication practises of these service providers need a total relook for respecting privacy as now defined by law. Every other day there is news of some breach of their subscriber records. Recall the last breach of Jio's subscriber records by a hacker from small town in Rajasthan. CERT-in reported 44,679 attacks in 2014 which have gone up to 50362 in 2016. Our ATMs were breached in mid-2017 compromising 3 million debit cards.Similarly, very often during last year, Aadhaar's based subscriber records at various Government offices has often been hacked. While Aadhaar is centralized in design and claims of all security measures at their end, in both the cases cited above,

Aadhaar's growing linkages with various state and non-state players have proved to be the weak link in the authentication chain. Needless to say, that this problem has to be overcome by defining secure standardized processes to be followed by all service providers using Aadhaar.

With growing use of mobile wallets and internet banking, banks too have to enhance their cyber security practises for protecting their data as also privacy of their users.

**Operating Systems and device manufacturers:**

They play an important role in bridging the last mile by providing devices and tools to access the Internet. But many of these also link up and stay connected to manufacturers' servers for service support, software upgrade and in a few cases for other covert reasons. Data being a strategic asset, very rightly Government of India has sought responses from all mobile manufacturers about cross-border data sharing. This challenge will soon become bigger with IOT coming into play. Such vigilance is needed for enforcing cyber security at national level. In the process, privacy too will be addressed.

**Need a Data Protection Law:**

Continuously evolving technology is resulting in paradigm shifts in the digital world at a rapid pace. At the same time, because of its vast and ever evolving scope, it is difficult to define privacy in straight jacketed legal vocabulary. It calls for defining sensitive legislation for data protection and right to privacy that is geared to assimilate such rapid changes in technology in a manner such that it does not throttle innovation and creates opportunities for economic growth. Hence, need of the hour is to define a Data Protection Law that is sensitive about defining extent to which individuals can exercise control over their personal data. Industry's interface of such data with the digital world during process of collection and portability for any kind of data processing / analysis has to ensure that user's privacy is not compromised.

Privacy rights needs to fully address individual's autonomy and consent in a manner such that it safeguards against unlawful surveillance. As stated by Mr. Milind Deora, Former Union Minister of State for Communications and Information technology, national law enforcement agencies cite "existential terrorist threat" as an argument for rejecting right to privacy. The state needs "to strike the delicate balance between safeguarding national security and Sovereign interest and ensuring that individual privacy is not imperilled….. Lawful mechanisms can be adopted to intercept terrorist threats rather than subscribe to a blanket surveillance policy."

This brings forth the need to introduce accountability into the process with legal redressal being available for any violation of privacy where offenders are brought to justice – the topic that is addressed next.

**Needed a National Authority/Commission for Data Protection and Privacy:**

In a rapidly changing economic environment due to digitization resulting in a connected world, security of data and privacy of user are of paramount importance. India's digital economy has to generate trust and confidence between the service provider and its clients in a manner such that it leads to increased usage of such privacy secure services – consequently resulting in innovations that generate more employment and economic growth. With Government too being involved with the roll-out of Aadhaar and various other services linked to it, it alone cannot be counted to be an arbitrator and guardian of privacy. Without checks and balances that are an integral part of

democratic functioning, as an involved party Government of the day could be prone to bringing out a draconian law (just as the Government had done while introducing Aadhaar without parliamentary sanction or has so far been interpreting privacy to its convenience). Accountability of all players in the digital arena has to be created for better governance.

A dedicated, independent, autonomous Authority with a well-defined mandate for data and privacy protection needs to be set up at national level reporting only to the President of India. It should have a complete oversight for implementing the Privacy and Data Protection Law. This organization should interact with Government, industry and users to oversee observance of fully secure data integrity practices. They should also enjoy legislative backing to look into complaints, investigate breaches through comprehensive audit and layout corrective course of action with mechanisms for redressal thatneeds to be implemented.

Such an organization should not only address data security needs of the individuals but also address potential threats that exist on sovereign data - repercussions of which could be economically very harmful to the nation. A national infrastructure needs to be built for implementing strong privacy regulations as a defence against all kinds of cyberattacks – both from within as also from across the border.

This organization should have judicial powers to prosecute and punish violators of privacy and data security norms as defined by the law.