Indian Supreme Court Judgement and the Re-birth of Privacy

SIGNZY

The landmark judgment

On 24th August 2017, a nine-judge Supreme Court Bench unanimously ruled that individual privacy is a fundamental right. The court noted that:

The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.

The right to privacy verdict, although primarily passed on a petition filed about the Aadhar Card scheme, will impact every company that collects and handles user data.

In its 547-page judgment, the Supreme Court touched upon the different aspects of informational privacy — and explained how collecting data could threaten an individual's privacy.

SIGNZY

Is Privacy a Right?

In 2012, Justice K.S. Puttaswamy (Retired) filed a petition in the Supreme Court challenging the constitutionality of Aadhaar on the grounds that it violates the right to privacy.

During the hearings, the Central government opposed the classification of privacy as a fundamental right. The government's opposition to the right relied on two early decisions—MP Sharma vs Satish Chandra in 1954, and Kharak Singh vs State of Uttar Pradesh in 1962—which had held that **privacy was not a fundamental right.**

SIGNZY

60 years in the making

The right to privacy in India has developed through a series of decisions over the past 60 years. Over the years, inconsistency from two early judgments created a divergence of opinion on whether the right to privacy is a fundamental right.

The 2017 judgment reconciled those different interpretations to unequivocally declare that it is. Moreover, constitutional provisions must be read and interpreted in a manner which would enhance their conformity with international human rights instruments ratified by India. The judgment also concluded that privacy is a necessary condition for the meaningful exercise of other guaranteed freedoms.

Applicibality

This Supreme Court ruling is a check: For both the government (against which the case was mainly fought) as well as the non-state actors or private companies because it doesn’t just oppose any privacy invasive practices employed by the government but also applies to private companies that collect user data.

It is the foundation for the Personal Data Protection Bill.

SIGNZY

What data is protected?

The information must be **“personal and confidential”** to be protected by right to privacy. One of the points raised by the opposing counsel during the trial was that privacy was vague and ill-defined. The judges patiently tried defining what is “private” data, to carve out the scope of law.

For example, the Court pointed out that data about electricity consumption pattern of a person is NOT personal or confidential, and couldn’t be protected as “private information”. That said, the Court also cited a UK judgement that stated the storing of the biometric data indefinitely of individuals no longer suspect of criminal activities would be an invasion of privacy. Clearly, a person’s biometric data is both “personal and confidential”.

SIGNZY

Relationship with Aadhaar

the Indian Supreme Court has ruled that India's controversial identification system Aadhaar is Constitutional. They based their conclusion on notes that there are sufficient measures in place to protect data, and that it is difficult to undertake surveillance of citizens on the basis of Aadhaar.

The court has demanded that the Government introduce a 'strong data protection law' as soon as possible. It also requires that Aadhaar not be required for some services, including for people applying to get a SIM card for their mobile phone, for opening a bank account, for government grants, and schools. The court also seems to state that use by the private sector must be limited.

The court also established a hard retention period -- previously the government kept authentication transaction logs for five years, and the court believes that six months is sufficient.

SIGNZY

Digital Privacy

While the court had a broader mandate and covered privacy from all aspects,they did cover digital privacy in detail. At some level they felt the real challenge to privacy is coming from this rapid transformation of processes from offline to digital.

The court stressed upon properties of the digital world that make it difficult to detect privacy invasion and hence heighten privacy concerns:

- Non-rivalrous — simultaneous use by multiple users
- Invisible — invasions of data privacy are difficult to detect — and it travels at speed of light making it further difficult to trace any breach of privacy. Data can be accessed, stored and transmitted without notice
- Recombinant — data collected can be used, analysed and combined to create more data output which is unseen earlier

SIGNZY

7-point framework to guide companies' data policies

From analysis of the judgement, a simple 7-point framework that shows the key points that organizations need to think about when framing their data policies was created :

1. **Personal vs Private:** Every data that is personal is not necessarily private. A user's name, for example. Because a person's name is used in public communication, name can be considered to be non-private personal information. Also any information that is anonymized is neither personal or private and exempt from purview of the law.
2. **Explicit Consent in plain words:** User's consent has to be taken explicitly and cannot be hidden inside lengthy terms of service or agreements.

SIGNZY

7-point framework (Contd.)

3. **Consent alone is insufficient:** Court has also opined that in certain situations, even a consent based mechanism may not be able to protect the customer and hence encroachment of privacy shouldn't be a preferred option.
4. **Necessity:** This is a simple principle which asks the question if collecting it is really necessary to invade privacy to achieve the outcome.
5. **Proportionate benefit or risk:** Whenever it is necessary it should be weighed against proportionate benefits and risks. Privacy should not be encroached unless there is some proportionate good possible or some bad that is preventable.
6. **Right to Forget:** Eventually the user should have the right to revoke access to his/her data
7. **Access and Correction:** The ownership of data is with the individual whose private data is collected. Therefore he has a right to access and correct the data or delete as given above.

SIGNZY

Impact on Financial World

1. **Credit History under Credit Information Act**

- Collection of credit data: Collection of credit data by the creditor is completely ok as it is consent-driven private data between the two parties.
- Exchange of credit data: Banks report credit data to licensed agencies. These agencies then exchange this data with other banks as requested by the bank. This might require clear exceptions made in the privacy act or a re-look into how credit reports are requested, what kind of information can be shared and what is to be hidden.
- Access and control over credit history: Currently consumers cannot easily request credit history to be forgotten or edited. Going further there would need to be an option to have greater control and access of one’s own credit history.

SIGNZY

Impact on Financial World (Contd.)

2. Pulling data of a customer from KRA by Mutual Fund and AMCs

- Collection of data: Currently the agency that collects the data and the one that stores the data are different. Clear consent and declarations hence maybe needed.
- Current practice of data pull from PAN, without an appropriate consent layer may also need a relook.

3. Account Details

- Login based scraping: Account username and password definitely fall into the domain of private data. And the reason in many cases is convenience, as it might be more difficult for the user to submit a copy of bank statement himself. Thus this encroachment may not meet the principle of necessity or proportionate benefit.
- Account Aggregator: The new RBI guidelines provide for a consent layer and a lot of regulation around security of such data. The data does not remain with the aggregator post-completion of the purpose and therefore the guidelines seemed to have given protection to privacy and may not be greatly affected by the judgment.

SIGNZY

Impact on Financial World (Contd.)

4. Mobile data collection during application download

- Malware or Security risk: The data collected to assess malware risk may not fall within privacy parameter. Specially if it can be anonymized enough to be unlinked to the individual himself. But current assessment tools and processes might need to ensure they follow this principle.
- SMS reading: This is being seen as a new innovative way to provide credit assessment. But within the new privacy regime, this maybe really tricky. Let us explain: SMS reading is a clear invasion into privacy and hence would require explicit consent. But where it gets really tricky is that SMS is usually a private conversation between two parties and hence you would need consent of both the parties to read SMS. It will be interesting to see how the innovation can be enabled without being unlawful.
- Reading personal contacts to use later for collection: Like SMS reading this may also need consent of two parties and hence should be seen in the same light. (Signzy would be coming up with another article on multi-party conversations including email, sms, call etc. We will examine in detail the implications under a privacy law.)

SIGNZY

Impact on Financial World (Contd.)

5. Aadhar based KYC regime

- There are two KYC possibilities in Aadhar A) Demo Auth B) eKYC — biometric or OTP. As the Aadhar regime has a robust consent architecture in place it should hold good even in the present regime. The only concern raised by the court was on biometrics being private. Hence the nature of benefit should be proportionate as consent alone, as noted by the court may not be enough protection. Hence biometric based KYC for account opening, new SIM or other risky scenario might be acceptable. Biometric based KYC for non-risky scenarios such as event registration might need a relook.
- The other more grave change maybe the need for an alternate option. While the financial regulators in line with government view had been pushing a biometric KYC, the current law would require the financial system to provide alternatives. This is especially true for cases where there maybe no real risk or proportionate benefit of forcing biometric KYC.

SIGNZY

References

https://blog.signzy.com/sc-judgement-and-the-re-birth-of-privacy-3d2fcf1201dc

https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar

https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time

SIGNZY

For more information visit us at:

: Signzy

: signzy.com

: @TeamSignzy

: /TeamSignzy/

SIGNZY