Strengthen Aadhaar With Privacy Law

Welcome court ruling on right to privacy

The Supreme Court's nine-member Constitution bench has found, unanimously, that the right to privacy is a fundamental right, arising from the working, jointly and separately, of the Constitution's Preamble and the fundamental rights listed in Part III. This removes ambiguity on the subject arising from conflicting past judgements on the subject. It also provides a five-member bench hearing a challenge to Aadhaar, the biometrics-based unique identity scheme that has already enrolled more than a billion Indians, a firm basis for evaluating the challenge on the basis of Aadhaar's breach of privacy.

True, the current ruling proves wrong the Attorney General's contention that the Constitution does not offer a fundamental right to privacy. But this, in no way, erodes the case for Aadhaar. All of India's fundamental rights are qualified, none is absolute. So would the right to privacy be. On reasonable grounds, and with the due process of law, the right to privacy can be breached. The benefits that Aadhaar holds out are immense, from efficiency in government expenditure to preparing against threats ranging from epidemics to terror. The costs stem from the potential for misuse of Aadhaar data. The point is to bring in robust legislation to prevent misuse of individual data either by the state or by non-state agencies. India can bring one law for each or a combined law on data protection. An independent regulatory body answerable to Parliament should be put in charge of enforcing data protection and ensuring that no use is made of a person's data that brings him or her harm.

Data is valuable. As the Internet of Things and greater social media penetration generate zettabytes of data, analysing this data to produce actionable insights would become a huge and lucrative business. Artificial intelligence calls for masses of data, for training algorithms. For India to gain from these fields, we must enact robust data-protection laws harmonised with similar laws in other jurisdictions. To advance civil rights and economic opportunity, we need robust data protection.

Seeing Rail Safety as a Systemic Factor

Yet another rail accident points to the pressing need to revisit the issue of safety from an organisational perspective. As former General Manager Sarabjit Arjan Singh said on this page (February 11, 2017), the Railways must move away from inquiring into the chain of events that led to an accident to identifying what, in the structure and functioning of the organisation, led to decisions that produced the accident. Human error is identified as the culprit in most inquiries. But why do Railway humans err repeatedly in this disastrous fashion? Does the Railways specialise in recruiting bad apples?

In the recent Utkal Express derailment, the tracks under repair were not closed for traffic, and the train was allowed to speed along. In the Kaifiyat Express accident, a dumper was left on the tracks. A culture of safety is conspicuous by its absence. Once the Railways operate more trains than the tracks can handle, complete with the capacity reduction that accompanies periodic track repairs, its minders are constantly called upon to make trade-offs between safety and making the trains run on time. Block off traffic, so that the track can be repaired thoroughly, or do a hasty job of the repair so as to spare Railways the flak for late trains? If someone gets the trade-off wrong, it is easy to send him off on leave or premature retirement. But what of the decision to allocate less money to extending track capacity and more to running new trains, while the overall budget for investment stands constrained because of the fear of raising fares? There is little point in fixing blame on some individuals.

Just as sending a hundred satellites into space makes India's brand value rise, frequent rail accidents dent it too. It is in everyone's interest to overhaul the culture of the Railways to make safety an integral part of all decisions.

Automated and economical officiating clerics are the best bet for all religions

Why Not Rituals With Robotic Precision?

That technology and automation often have a disruptive effect is well established; that they also usually fulfil an economic or societal need is also obvious. So, the invention of a robot to take on the mantle of a priest for funeral rites in Japan and another one to bestow religious blessings in Germany, were almost inevitable. Populations there are ageing but still quite traditional. As the countries are prosperous, there not very many people would be willing to take up priestly duties — a comparatively modestly paid profession. Robots appear to be the perfect solution, as they can be expected to deliver word-perfect, on-time performances, at a fraction of the fees of their human Japanese counterpart.

The opportunities for India are obvious. Priests officiating at rites from birth to death are of varying competence here, and people are often unsure if rituals are performed as per the scriptures. Nor are the clerics of any religion very well paid. Given the country's rising prosperity and aspirations, an availability crisis is inevitable if not imminent. Robotic priests, well-versed in every religious rite prevalent in the country, could go a long way in addressing this issue. Of course, some may quibble about the robots' eligibility to officiate, but in these days of caste and gender equality, such arguments may not prevail.

RIGHT TO PRIVACY The verdict is the first step to ensuring our personal information remains out of bounds to anyone else

PRIVACY PUBLIC LTD

Outgrowing the Mai-Baap State

Samraat Basu & Sanjana Srikumar

A nine-judge bench of the Supreme Court unanimously found that there is a fundamental right to privacy under the Indian Constitution. The decision came in context of the Aadhaar scheme, which, among others, was challenged on the ground that it violated the right to privacy.

In consideration of different interpretations regarding the status of this right, a reference was made to this bench, which concluded that the right to privacy is an essential part of the right to life and liberty under Article 21. Further, aspects of this right may be present in other rights as well. Its implications within the Aadhaar case remain to be seen. However, the implications of this right extend far beyond that framework.

The right to privacy implies that there is a core of human personality that must be free from intrusion. An individual must have the autonomy to make decisions. This places the source of this right in the Constitution rather than statute. Second, it allows for new kinds of protection. For instance, in situations of marital rape or rape of male victims, the State may now need to justify its failure to protect victims from violations of bodily autonomy.

An important implication of this autonomy is on the protection of the rights of LGBTQ+ persons in India. Justice D Y Chandrachud has opined that sexual orientation is an essential attribute of privacy, and that the protection of sexual orientation lies at the core of the fundamental rights guaranteed by Articles 14, 15 and 21 of the Constitution.

This observation is significant since the question of Section 377 of the Indian Penal Code will be re-examined by a five-judge bench. Other possible implications could be on the use of court-mandated medical examination or polygraph tests, adding to the right against self-incrimination.

The second implication is on the question of civil liberties. Chandrachud has also expressly overruled the decision (made by his father, Justice Y V Chandrachud, in 1977) in the 'ADM Jabalpur v Shvakant Shukla' case, and held that life and personal liberty are primordial rights that are inalienable to human existence. So, the construct that by adopting the Constitution, the people of India surrendered the right to life and personal liberty to the State, on whose mercy these rights would depend, is manifestly expelled.

Third, there is a protection for communication and manifest conduct, which must be free from State surveillance. This recognition has already been granted by the courts in cases of wiretapping of phones. In recognising the right to privacy, such a result would exist in all cases of state surveillance, whether or not the user is aware of the surveillance and irrespective of any demonstrable effect.

Finally, informational privacy also casts an obligation on the State to form a data protection law, which will address data privacy issues balanced with other legitimate State concerns, such as national security and optimum deployment of resources. This is a prerequisite of the digital age where individuals are constantly generating data. A pressing need for such a law is magnified due to the immense commercial value of the data generated by everyday digital activity.

Although the right to privacy has been formally recognised as a fundamental right, it is under no circumstances, an absolute right. Chandrachud has noted that there may be situations in which other legitimate State requirements may override a right to privacy.

However, such a restriction of a fundamental right to privacy must be justified by a robust regime that ensures the fulfilment of a three-tiered test: the restriction must be provided by law, in pursuance of a legitimate aim, and is proportional to the object and needs sought to be fulfilled by such law. Nonetheless, the decision remains significant.

The writers are research fellows, Vidhi Centre for Legal Policy

GoI to Prove It Can Keep Your Secrets

Nishit Dhruva & Khushboo Shah

The Supreme Court declaring privacy as a fundamental right is in consonance with the Right to Freedom. Privacy is a part of individual liberty and no person shall be deprived of privacy without due process of law.

At the same time, however, the Right to Privacy will have its own limitations and it can't be an absolute right in itself. A person has the right to determine what sort of information about them is collected, and how that information is used.

The first task for the authorities will be to interpret and fine-tune all the domains where the issue of privacy is involved. Second, a robust mechanism must be created to ensure this fundamental right is ensured to each one of us. The first task will take care of the ambiguities in the rules, while the second will address the loopholes. Privacy cannot have an inclusive definition till we list out the dos and don'ts.

The biggest implication of the judgement will be on the Aadhaar row, which a five-member bench will now try to solve in the broad light of Thursday's verdict. The Centre now has to convince the Supreme Court that forcing citizens to give a sample of their fingerprints and their iris scan does not violate privacy. The biometric information shared during the process of obtaining an Aadhaar card — which includes not just the fingerprints but also a retina scan — could become the next big problem of 'stolen identity'.

While banks are still struggling against security breaches over credit card usage despite implementing state-of-the-art cyber security measures, GoI has to prove itself to be capable of handling the security of such confidential data and being able to maintain confidentiality.

The next crucial area is online privacy. In the light of today's verdict, internet users can protect their privacy by taking actions that prevent the collection of information. Protecting personally identifiable information is important for preventing identity theft.

As far as social media policies and practices are concerned, it has been a suo motu disclosure when someone uploads a video, makes a comment, shares his location or an article. They are never forced to do so. With the new technological developments, the issue of data sovereignty — the practice of subjecting information to the jurisdiction of data privacy laws on the basis of geographical boundaries — may act as a chink in the right to privacy verdict armour.

Today, data is moving seamlessly across globe, with no ownership over its storage. Unless explicitly specified, Indian IT laws are not applicable to data stored outside India and data intermediaries can claim immunity by exploiting this loophole.

This judgement will also leave an impact on India's ambitious path to evolve as a complete digital economy. The question now is how much personal information can be stored, processed and used by both government and private parties.

The right to privacy, being an intrinsic right under Article 21 of the Constitution that provides the right to life and personal liberty, must have penal provisions in place for its violations. When the right to privacy relates to cyber crimes, the Information and Technology Amendment Act, 2008, separately deals with provisions with regard to penalties and compensations.

An important concern relates to the modernising of penal laws in many countries that exist prior to the advent of computers. On the one hand, existing laws have to change to cope with computer-related fraud such as hacking, malicious falsification and erasure of data, software theft and software attacks, and on the other, a new legislation is also necessary to ensure data protection and piracy.

Dhruva and Shah are managing partner and associate respectively, MDP & Partners

Your Personal Data is Yours & Nobody Else's

Abheek Barman

Raise a toast to nine judges of the Supreme Court (SC) who have said your right to privacy is fundamental, ranking right up there with rights to life and freedom of expression. Privacy as a fundamental right probably didn't matter much in 1954, when the first anti-privacy judgement was delivered. It matters now, when companies like Alphabet (owner of Google), Microsoft, online retailers, Facebook and Twitter can snoop into your finances, links with family and friends, mails and opinions.

The SC order implies that your data belongs to you, not to companies or regimes. Big Brother regimes try to manipulate every thought and action of their citizens. The latter descend into a Stalinist hell of self-censorship, paranoia, spying and snitching on each other. In 1952, the Soviets worked out a telephone-based system that allowed a group of people involved in launching rockets and missiles, to communicate across vast distances via a phone network. This was the ancestor of the internet.

Fast forward to 2012, when Russia drew up its Internet Blacklist. Apparently, this was to protect children from harmful content, curb drug use and other evils. That was the fudge. Soon, it expanded to include sites 'inciting hatred', 'suspected extremism' and 'deviant behaviour' including gay relationships. By August 2014, a 'Bloggers' Law' came into force, where all Wi-Fi and chat-room operators had to collect users' data, verify their passports and store them. Social media was controlled by a complex thingummy called Deep Packet Inspection.

In July 2016, Russia passed the Yarovskya Law, forcing telecom operators to record and store all conversation, message and internet traffic for six months. This November, a new law will ban all software and websites that try to go around Russian filters. Phrases like 'Caucasus', 'Crimea' and 'Ukraine' are taboo; Bitcoin has been blocked recently.

All this operates under the System of Operational Investigative Measures (Sorm), which reports to the FSB, successor of the KGB. Sorm arm-twists telecom and hardware companies to allow snooping. It also mandates inspection, arrest and shutdown without warrants.

On September 20, 1987, the first email was sent out from a primitive system in China. It said, 'Across the Great Wall, we can reach every corner in the world.' What irony. In less than 15 years, a system called the Great Firewall (GFW) controlled all online traffic. In 2003, GFW spawned Golden Shield to monitor and censor content. All backbone providers are owned by the communist state.

Before it walked out of China, Google agreed to block searches on phrases like 'Tiananmen' or 'democracy'. Companies like Yahoo and Microsoft have bowed to all strictures of Beijing. Ironically, almost all the hardware that runs Beijing's spying machinery is outsourced from US companies like Cisco Systems.

Whistleblower Robert Snowden showed how the US' National Security Agency (NSA) spiced up its mandate to track terror by spying on US citizens, as well as those from friendly nations. Snowden's revelations implied that once data is centralised by the State, it is easier for online crooks to steal vast chunks of information. Financial information 'dumps' are sold on the Dark Internet, and used to hack into personal accounts or bank systems to steal cash.

In the last three years, India has lurched towards large-scale data snooping. Its primary vector is the Aadhaar ID number and card. The original idea was to stop subsidy leakage. It is now mandatory to have an Aadhaar number to file tax returns and open new bank accounts, enlarging the scope of financial fraud. Infants in Anganwadi crèches now need Aadhaar to get a midday meal. Never mind media reports that suggest that the Aadhaar system is about as secure as a sieve.

In Russia, phrases such as 'Caucasus', 'Crimea' and 'Ukraine' are taboo; and the government recently blocked Bitcoin

Petitions to rein in Aadhaar begged the question whether your data was yours or whether companies and governments could filch it. On Thursday, the Supreme Court made your right to privacy, including personal information, a fundamental right. We might yet pull back from the abyss.

MERGERS & ACQUISITIONS

Good Time to Join the Dots, Cross the T's

Karan Singh

We are on the cusp of a broad-based consolidation wave in Indian business. One has only to read the headlines to grasp the heightened level of merger and acquisition (M&A) activity across sectors. These big-ticket deals are driven by emerging opportunities and led by dominant players who are reshaping the industry structure within their sectors.

In telecom, the number of service providers has fallen from more than 10 to 4-5. The most recent merger proposed between Vodafone and Idea will create an entity with a combined enterprise value of an eye-popping $23 billion, making it the largest telecom company in India. Among old-economy companies, UltraTech Cement closed its $2.4-billion acquisition of Jaypee Group's cement assets. Even the relatively young e-commerce sector has been reduced to a two-horse race between Flipkart and Amazon.

The last financial year saw a record level of M&A deals, valued at $66.2 billion. This year promises to be even bigger. Incidentally, a majority of 2017 acquisitions have been domestic, rather than cross-border, deals.

What is driving this surge? And what lessons do these deals offer for corporates? There are four broad triggers behind the heightened action.

▶ Industry disruption: A prime example is of Reliance Jio, which compelled other telcos to respond so that they could remain viable and improve their market position — with a focus on increasing access to spectrum, retaining customers and weeding out duplicate costs to protect their operating economics.

▶ Distressed assets: Distressed assets are allowing stronger players to improve their strategic positions cost-effectively, as in the cement and power industries. Jaypee, for instance, has had to sell its cement assets to pare down its debt.

▶ Regulatory changes: Regulatory changes and moves such as consolidation of banks, notably the merger of the State Bank of India (SBI) and its associate banks, are the next big trigger.

▶ Overseas assets: Availability of reasonably priced overseas assets allows Indian players to solidify and expand their global strategic aspirations. They are doing this smartly by accessing cheaper overseas financing and benefiting from richer Indian multiples. Motherson Sumi's acquisition of PKC Group, the Finnish maker of automotive wiring systems, is a case in point.

These trends also indicate that the market is starting to mature. Companies are preparing to take advantage of the next chapter of growth and positioning themselves to capture a share of future profit pools. However, those considering M&A should weigh the following factors.

FILE PHOTO

Fitting right in

First, periods of turbulence are crucibles of both opportunity and risk, offering a chance to reshuffle decks. Bain data from the US suggests that during such periods, there is potential for companies to move up or down two quartiles in terms of market position. And for those changes to endure. Although the possible rewards are great for strong companies, weak players can make big mistakes: if not handled strategically or not well-executed, M&A actions may create lasting casualties.

Second, acquisitions that improve strategic leadership, undertaken by companies performing well, have higher odds of success. So, what are the economic rules for profit-making in the industry? Is it about being scale-driven (global, national or regional)? Or is it about share position in premium categories (consumer products), or access to proprietary assets, or resources that drive value creation?

Third, successful M&A deals are usually carried out by serial acquirers with a repeatable model, not by companies that make big bets infrequently. M&A moves by companies that have a weak core can also be disastrous.

Fourth, diligence and integration are both critical in ensuring success. To avoid getting caught up in deal fever and overbidding, companies need to establish a clear and strategic deal thesis and test it objectively during diligence. During integration, it is vital to follow the money and focus heavily on the key value drivers of the deal. It is equally important to customise the integration approach depending on company size and whether it is a scale or scope deal.

Finally, the importance of no-regret moves cannot be overemphasised. These include reassessment of strategy and rules of the game as industry dynamics change; a focus on strengthening customer loyalty and differentiation as competitive intensity increases; and, from a defensive point of view, a focus on achieving the highest level of cost-efficiency.

A superabundance of capital will contribute to the trend, with corporate and financial investors sitting on significant dry powder they can deploy. Armed with an understanding of today's M&A landscape, companies can leverage the unfolding opportunity for strategic boldness, and for forging a new path to economic leadership.

The writer is managing director, Bain & Company India