Financial inclusion and the right to privacy

As India uses Aadhaar to advance financial inclusion efforts, it is essential that both privacy and financial interests of the poor are protected. The Supreme Court in a landmark ruling on 24 August decided unanimously that there is a fundamental right to privacy in India. It called on the government “to examine and put into place a robust regime for data protection”. Legislation to protect the privacy interests of the poor should now be top of the agenda.

What should that legislation look like? Unhindered by the outdated and entrenched approaches to privacy in jurisdictions such as the US and Australia, India has the unique opportunity to put in place a model system for the governance of privacy, one that is far better suited for the digital age and for expanding financial inclusion.

A data protection law is especially important at this early stage in the development of databases, policies and systems in India that rely upon Aadhaar. While Aadhaar promises to bring improvements in the delivery of services to poor people and under-served communities, it could also facilitate the collection of massive amounts of information, which would expose vulnerable consumers to privacy risks—competing factors that well-crafted legislation can address.

Integration of Aadhaar into the economy helps the financially excluded to access life-changing loans, insurance, savings and payments services more easily, and the costs of the financial services delivery likely will fall as a result. Aadhaar can also help citizens receive timely and complete payment of their government benefits.

Yet, if government and the private sector collect Aadhaar numbers for everything from utilities to health services, from car insurance to residential leases and link the information collected from countless databases, Aadhaar could become the organizing tool for the compilation of sensitive, detailed and constantly evolving individual profiles. Corporations and government with access to these profiles could use them in abusive ways to describe, predict, and ultimately influence the behaviour of individuals, sometimes without their knowledge.

Data from a person’s purchasing history, location, habits, income and social media activity can be used to classify consumers and customize the price of financial products or the interest rates charged to them. Such customization could exploit the consumer unfairly, based on their habits, or enable financial service providers to discriminate directly or indirectly based upon the customer’s ethnicity, gender, caste or religion. Government access to profiles can also raise privacy concerns. The vast amounts of data generated by new technologies and linked to Aadhaar increase the potential for abusive data practices and privacy invasion. The Supreme Court’s ruling is a vital first step in responding to this danger.

Many countries base their data protection regimes on the exercise of consumer choice or “informed consent”. But putting the burden on consumers to read lengthy and legalistic privacy notices and then to exercise choice about how their data will be used is unrealistic anywhere in the world. How many people read privacy notices before installing an app on their phone? Apple’s privacy policy for India runs over 3,000 words. Microsoft’s privacy statement is well over 7,000 words. India can recognize the reality that consent is no longer practical as the primary justification for data practices and establish substantive privacy protections regarding the collection, use and disclosure of personal information.

India also has the opportunity to establish safeguards for consumer privacy that are integrally part of the design, including the technical design, of government and private sector systems. This approach, often called “privacy by design”, has received widespread support from regulators and

policymakers around the world. The European Union's General Data Protection Regulation (GDPR), which takes effect next year, mandates data protection by design and by default, significantly expanding the reach of this process.

A critical feature of any data protection regulation will be the limitations placed on the collection and storage of personal data. Some, in the US in particular, have advocated "use-based" systems of data protection regulation, which focus on permissible uses of data without restricting its collection and storage. However, the collection and storage of data should also be regulated, especially considering the vastly increased opportunities for harmful and unauthorized access the more data is collected and the longer it is kept, and the social harms created by pervasive surveillance.

The Supreme Court was not called upon to address all the ways Aadhaar might be used consistent with a citizen's right to privacy. These issues, including whether providing one's Aadhaar number can be made mandatory, will need to be decided in subsequent cases.

Judicial rulings are one path for developing the right to privacy. The legislative path allows India to develop world-leading data protection that moves away from the flawed notice-and-choice model to one that establishes for the government and private sector alike clear, predictable parameters on the collection, use, processing, sharing, and the security of personally identifiable information. The Supreme Court's recognition of a right to privacy provides the foundation to ensure that innovations such as Aadhaar are used to enhance the poor's dignity and well-being.

Katharine Kemp is a research fellow on the UNSW digital financial services research team, Faculty of Law, UNSW Sydney.

Comments are welcome at theirview@livemint.com

END