Article Title: “Aadhaar and data security: Irrespective of what one feels about Aadhaar, a comprehensive new privacy law is needed”

This article has been published in 'The Times of India' on 10th May 2017.

Shortlink:https://goo.gl/o3AnFI

Once again Aadhaar, India’s biometric identification system that is the largest such project in the world, is in the eye of a storm after being made mandatory for tax returns. The Supreme Court has started hearing a public interest litigation (PIL) challenging that, and both social and traditional media are abuzz with strong views on the topic.

I filed in Parliament, some weeks ago, a Private Members Bill on Data Privacy and Protection, and for much longer have been advocating the overhaul of our woefully obsolete and fragmented laws with a comprehensive new Act. But this is far from being a black and white issue, and there are many nuances that deserve more deliberation.

Though Aadhaar has become the focal point of this debate, threats to data security and citizens’ rights to privacy go far beyond it. In fact, as its creator and IT industry wunderkind Nandan Nilekani puts it, if a malicious hacker or secretive agency were to try hacking your privacy, cracking Aadhaar would figure low on their list of ways to go about it.

There is vast information about us already out there in the cloud, including biometrics, with more collected every day. This happens through malware, covert eavesdropping, and the mindless permissions we voluntarily grant social media sites and apps. There is now a growing global movement to treat data as one of the world’s most valuable resources and, just like oil was a century ago, tightly regulate it in the public interest.

And just as antitrust laws were passed in the US more than a century ago to break up the dominant Standard Oil Company, now even that flag bearer of free markets, the Economist, has endorsed a call to break open the data dominance of internet giants like Google, Amazon, Apple, Facebook and Microsoft. But even ardent trustbusters recognise the immense benefits such companies have developed for humankind and expressly seek to preserve those, aiming only to prevent the abuse of dominant power.

By contrast, many pro-privacy and data protection activists in India are largely in denial about the benefits of Aadhaar, while correctly seeking to plug the threats related to it. Ironically, when it comes to other risky aspects of our growing connectedness, such as online financial transactions, even the most passionate activists seek reasonable security measures, not outright bans or curtailment.

Our approach to Aadhaar must be the same, taking advantage of its immense potential for good while putting in place a modern legal framework to prevent abuse. Aadhaar has already led to the plugging of significant ‘leakages’, a polite term for massive corruption, but the potential is far, far more.

Many people remember late PM Rajiv Gandhi’s 1980s comment that only 15 paise of every rupee spent by government ever reached beneficiaries. Newer data from the

erstwhile Planning Commission between 2005 and 2014 revealed that 40-73% of the money spent on the public distribution system (PDS) never reached beneficiaries.

Similarly, mind-boggling amounts of taxes are evaded in India by the simple tactic of maintaining multiple permanent account number (PAN) cards, which are required for bank accounts and big transactions. India has approximately 19 million income taxpayers versus 250 million PAN cards, and there is no way to de-duplicate the latter without Aadhaar. There are several such examples of large-scale fraud or inefficiencies that could also be cleaned up.

The conflation of alleged leakage of Aadhaar numbers as leakage of the underlying biometrics may be confusing to some. Nevertheless, whether cavalier or criminal, such misuse of private data is unconscionable and should attract punishment. In any event, irrespective of what one feels about Aadhaar, a comprehensive new data protection and privacy law is needed to supersede the inadequate and overlapping Indian Telegraph Act (1885), as well as the Information Technology Act (2000) and its Rules (2011).

The data protection aspect of such a law must emphasise a person's rights to her personal data; require her informed consent to collect, process, remove or alter such data; oblige those who deal with data to keep it secure; and have a grievance mechanism to punish violations with hefty fines and imprisonment.

However, the privacy aspect of any new law is bound to be complex and will undoubtedly stir even more controversy. Indian laws don't provide for a specific right to privacy, though court judgments have defined certain limited rights, and the SC has admitted yet another PIL on the topic.

Meanwhile, some activists' insistence on citizens' absolute right to privacy will inevitably run afoul of security considerations, including in some cases national security. In this age of terrorism, the issue of surveillance will be a major point of debate. Standards will be needed which permit the anonymous surveillance of metadata, such as algorithms that flag frequent references to, say "RDX" in emails, with prima facie evidence and warrants being required for further snooping.

Like it or not, we have already ceded rights to absolute privacy, such as with body scanners at airport security, not to mention widespread adoption of CCTV cameras. New technologies enable these to have biometric capabilities too, allowing individual identification similar to Aadhaar.

That should not mean more concessions of privacy are to be wantonly permitted. But neither should it mean the imposition of unreasonable, impractical rules that thwart 21st century life.