FINANCIAL EXPRESS, Delhi, 30.11.2017
Page No. 8, Size:(9.88)cms X (13.49)cms.

Protecting privacy

Srikrishna panel offers some solutions, solicits comments

THOUGH MOST DISCUSSIONS in the current surcharged atmosphere tend to equate 'data protection' with just Aadhaar, as the Justice BN Srikrishna panel on this brings out, there are many more facets that need to be dealt with. The fact that some government departments have inadvertently leaked information about people's names, addresses, bank accounts and Aadhaar numbers—though never the actual biometrics that reside in the Aadhaar database—is certainly worrisome, even if the Aadhaar Act tries to protect against this. But what about the fact that almost every app you download wants access to your phone calls, directories and calendar—should this be allowed? And when that data is sold to someone, or processed by, say, a Google to get consumer insights, do consumers have the right to ask for their data not to be included, or for them not to be targeted by advertisers/marketers based on this information? People worry about Aadhaar data being used to profile them—since the taxman, banks, credit card companies, etc, are governed by their own confidentiality rules, this is difficult—but don't think much about how this can be done through the apps they use every day.

While Srikrishna offers tentative solutions, it has put these out in a white paper soliciting comments—for instance, should all the data being collected by a Google about Indians reside in Indian servers or can they be located in the US? Since data protection is different for each type of data, Srikrishna starts off with the very basic user-consent being essential—as Aadhaar is mandated by the law, the consent here applies to allowing government departments to make your details public. Most apps, of course, get user consent through lengthy/confusing consent forms and, in any case, users have no option but to accept them in order to be able to download the app—the panel suggests a short and simple form to avoid 'consent fatigue'. It suggests a Data Protection Authority to draw up guidelines for each organisation—like a WhatsApp or a Google—to follow, and a Data Protection Officer in each organisation whose job is to ensure the guidelines are followed; if, for instance, the Authority says most apps don't need access to your phone records, it will need to ensure this is being followed. The Authority could also conduct Data Protection Impact studies and assign Trust Scores to each app/organisation which would be of great help to users. There could be, perhaps, even be a Consent Dashboard, where users can see where their data is being used... Though it sounds easy to say all data must be protected, as Srikrishna brings out, this is a complex, and constantly evolving task—and no matter how many rules are laid out, decades of legal challenges/suits will also play a role in how this finally pans out.