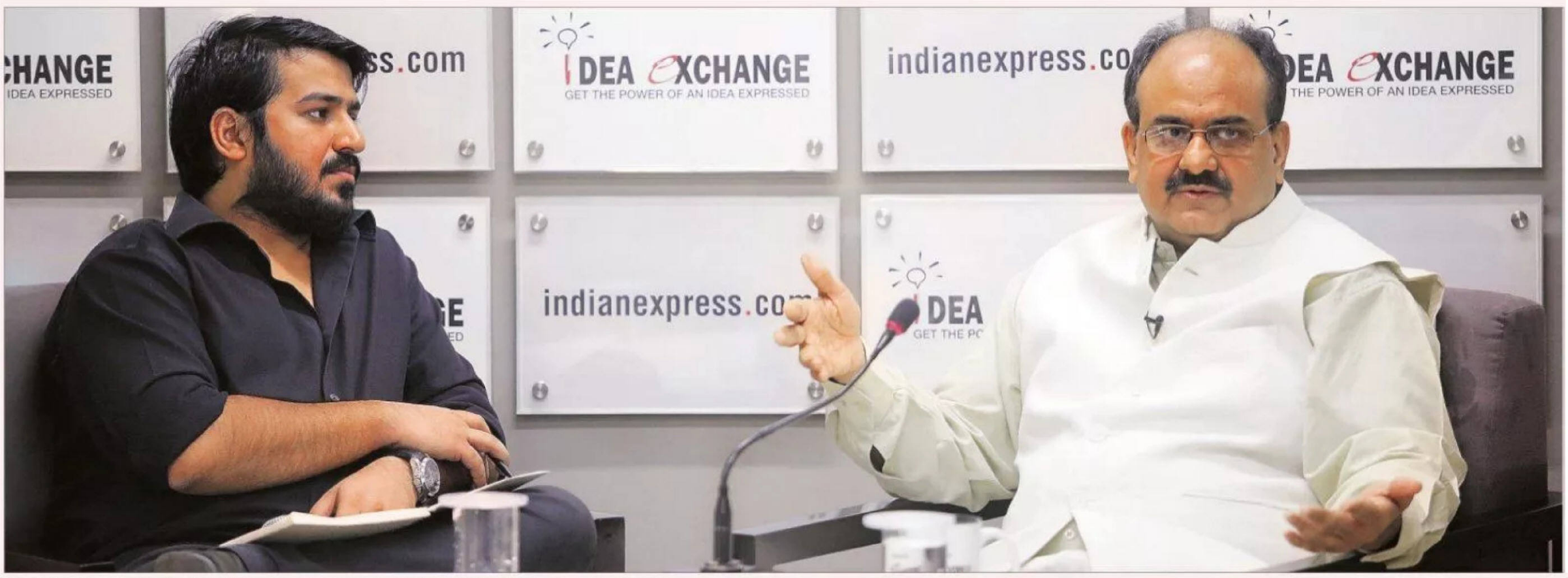
INDIAN EXPRESS, Delhi, 20.5.2018
Page No. 16, Size:(37.24)cms X (51.45)cms.

UIDAI won't know, say, if one has a car... Even if national security is invoked, it can't tell you this

Unique Identification Authority of India CEO Ajay Bhushan Pandey rules out surveillance through Aadhaar, denies beneficiary profiling by State Resident Data Hubs, assures action against entities misusing the unique ID, explains why EU's Data Protection Regulation is not applicable to India, and insists UIDAI is open to criticism



UIDAI CEO Ajay Bhushan Pandey with principal correspondent Krishn Kaushik in *The Indian Express* newsroom

PRAVEEN KHANNA

KRISHN KAUSHIK: The Srikrishna Committee white paper pointed out the need for a data regulator. Can Aadhaar and the Unique Identification Authority of India (UIDAI) come under such a data regulator?

We have multiple regulators in our country, and the UIDAI is also one of the regulators. The UIDAI regulates all that is concerned with Aadhaar enrolment or Aadhaar authentication. The regulation happens under the Aadhaar Act. But certain areas are outside the ambit of the Act. I don't believe any regulator is under or above any other regulator. Each will have its own role, and each will have to work under the provisions of the respective laws framed for them.

Let me give you an example. The RBI is the regulator for all financial data. So, the RBI will continue to do the job that it is supposed to be doing under the Banking Regulations Act. But the areas not covered under the Banking Regulations Act will come under the data protection Act. Similarly, the areas not covered under the Aadhaar Act will come under the new data protection Act. So, in relation to these areas, the rulings of the data protection authority will apply to the UIDAI, RBI or any other regulator.

KRISHN KAUSHIK: One of the main arguments against Aadhaar is that it can be potentially used for surveillance.

We have a very strong Aadhaar Act which rules out the possibility of surveillance through Aadhaar. Compared to any other contemporary law, the Aadhaar Act has a much higher level of safeguards to protect privacy and avoid the possibility of surveillance. For example, when it comes to tapping phones, there are regulations which allow only some government officers to authorise it. For Aadhaar, this has been raised to the level of cabinet secretary. There is a committee chaired by the cabinet secretary which also includes the law secretary and the IT secretary. Only they can permit usage of Aadhaar or biometrics in case of a national security issue. The use of Aadhaar or biometrics is completely out of bounds even for the courts.

In one case, the CBI wanted the biometrics of some residents of a certain state to figure out who had committed a crime. So the CBI sent us a legal order from a magistrate. It was challenged. Then they got an order from the high court and we challenged that too. Finally, we got a stay from the Supreme Court. At the time, the Aadhaar Act was not there but even then we were very clear that the biometrics and other information that we are holding, are not the UIDAI's data but the data of the people. We are only a custodian of that data and we cannot use it for any other purpose other than the one that was declared to the people.

Just a few months ago, we got a case from the Madras High Court: former chief minister Jayalalithaa's fingerprints were asked for. We politely told the court that under the Aadhaar Act, we are not permitted to give biometrics to anyone. That is the level of protection that has been built into the Aadhaar Act.

So what happens if somebody misuses the data? Any unauthorised disclosure of biometrics or any other information from the UIDAI is a criminal offence and punishable with three years imprisonment. No one is exempted. If my own employees do it, or even if we do it, we will also be subject to criminal procedure.

KRISHN KAUSHIK: The UIDAI had signed contracts with some states to produce State Resident Data Hubs (SRDH). In light of that, some states are using the Aadhaar data for 360 degree profiling — it is being called SRDH Plus.

If a state government is giving certain benefits to somebody, they need to know that person's identity, and whether they meet the criteria for availing that benefit. The information has to be collected through various sources — Aadhaar can also be used. It is not profiling; it is checking eligibility. As long as Aadhaar is being used for it (checking eligibility), it is fine. But if it is used to find, say, political preferences, information on caste or religion, then it is a serious matter and the issue will have to be brought up before the law.

PRANAV MUKUL: What kind of safeguards do you think are needed to stop profiling by commercial entities?

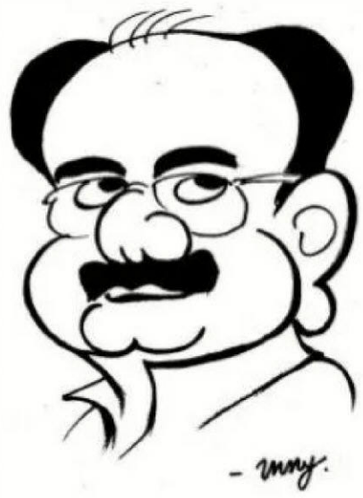
Not just Aadhaar, none of your personal information should be published. One can be profiled on the basis of one's mobile number... When we talk about personal data protection, including Aadhaar number, it should not be put out in the public domain. If somebody does a Google search of a mobile number and gets data from various sources, that is also a kind of profiling. We should not allow that to happen. This is the purpose behind giving 'sensitive' status to Aadhaar numbers. It means that we recognise that this is a unique number and should not be put out. But, at the same time, it should be usable and must allow one to establish one's identity. Therefore, the entities that are using Aadhaar should be sensitive and responsible. If they publish the data, and we find that they are doing so intentionally, then we will take action against them.

SEEMA CHISHTI: This massive seeding of data in one place is happening on the fundamental principle that all citizens are hiding something. How do you address that problem?

The Aadhaar system was designed on the basis of minimal data and optimal ignorance. When we actually do Aadhaar enrolment, you may have noticed, we do not ask for the father's name or the mother's name. Only your name, address, gender, date of birth, photograph, 10 fingerprints and the iris scan are required. Caste, religion, income and so on are not needed. On the other hand, when you apply for, say, a mobile SIM, you give out a lot of information.

For example: when you go to get a SIM card and you give your Aadhaar number and put your fingerprint, what we get from the telecom agency is just the Aadhaar number and the fingerprint. Then, we either tell them a 'yes' or a 'no', or we send them an electronic copy of your Aadhaar card, which again has minimal information. This is what we call optimal ignorance. We don't know what SIM card and what number you are getting from the telecom company. We don't know who you are talking with using that SIM card. We also don't get any of the details you might see on Truecaller.

WHY AJAY BHUSHAN PANDEY



EARLIER THIS MONTH, the Supreme Court reserved its verdict on a clutch of petitions challenging the Constitutional validity of the 2016 Aadhaar Act, following a marathon hearing that lasted 38 working days spread over four months. However, concerns over data protection and failure of authentication persist. As the chief executive officer of the Unique Identification Authority of India and member of the Srikrishna data protection committee, Pandey is at the centre of the data security debate. The 1984-batch IAS officer insists that although no technology is 100% secure, all Aadhaar data is safe and cannot be used for any surveillance. In September last year, Pandey was also appointed chairman of the Good and Services Tax Network

MOHD UJALEY: From May 25, the European Union will enforce the General Data Protection Regulation (GDPR), which basically envisages 4% penalty on revenues if there is a data breach. Do you support such regulation in India? And what is your view on the GDPR?

Many such issues have been discussed in the Justice Srikrishna Committee. We feel that a law should be implemented with deterrence. Otherwise, you make a law but it is not followed. The GDPR is one of our inputs. In the Justice Srikrishna Committee, we studied data protection laws of different countries. We looked at what the situation is in the US, Europe and other parts of the world, and then discussed what is the system that will suit our country. The GDPR has many things that won't be applicable here and, maybe, we would like to do it differently. We will have to await the decision of the Committee.

> In Oct 2017, the Centre instructed that benefits not be denied due to failure of Aadhaar authentication. States were told to keep an 'exception record', for whenever alternative verification was used

KRISHN KAUSHIK: Aadhaar authentication failures have led to a lot of exclusion at the ground level.

If you read the Aadhaar Act, there is one section which is very critical — Section 7. This Section is used by the Central and state governments to make Aadhaar mandatory. The Section states that the Central government may require Aadhaar authentication for delivery of benefits, services or subsidies flowing out of the Consolidated Fund of India. Earlier, the benefits would be taken by someone who isn't eligible or sometimes non-existent... The Central government can make Aadhaar mandatory, but, as with any technology, it may not always work 100 %, particularly when you have layers of technology. When somebody goes for Aadhaar authentication, maybe the device at the site isn't working at the time or maybe there is a power failure or a telecom failure or maybe the biometrics, like fingerprints, are worn out. We were quite aware of this fact. So, what we provided in the Aadhaar Act itself is that if the authentication fails, then the person can prove his identity by producing the Aadhaar card and going through some other procedures and avail the benefits.

Off and on, we do get complaints that a person's biometrics didn't work and he was denied benefits. We have communicated this to the state governments and Central ministries. In October 2017, the ministry of consumer affairs, food and public distribution wrote to all state governments stating that no one should be denied benefits due to authentication failure. Instead, they were asked to keep an 'exception record' and mention that one person failed the authentication and, based on alternative verification, the benefit was given. The 'exception register' should also not be misused, or else the whole system will become non-functional.

KRISHN KAUSHIK: What is the authentication failure rate?

I presented this information in the Supreme Court. What does authentication failure rate mean? We have three broad categories of users. In the telecom segment, crores of people have got authenticated — the fingerprint authentication rate is 97%. At banks, the fingerprint success rate is around 94-95%. Then, there is the Public Distribution System, MNREGA, where the success rate is 89%.

While analysing this data internally, we figured out that there is a difference in all categories. We can't say all users in telecom have good biometrics therefore the success rate is high. Even manual labourers use telecom connections, old people also need them. So, the population sample would be the same across the three broad areas. Then, why is there a difference in the success rate? One of the initial feedback we got is that in telecom, the SIM card agent wants to sell his SIM and so he properly guides the customer. So the success rate is high. It is the same with banks.

When it comes to government schemes, there are problems of massive leakage and corruption. In these places Aadhaar is upsetting legacy interests and so there is some initial resistance. Here the success rate is a little lesser. But we have also seen that, over a period of time, even those who want to defeat the system, come around and join the system.

SUNIL JAIN: You mentioned that in the time of a national emergency, if the cabinet secretary decides that some data needs to be disclosed, it will be disclosed. Can you disclose someone's biometrics?

If for national security reasons they ask us to provide biometric data of a certain terrorist, or if they want information on the number of places a particular Aadhaar number was authenticated... this is the kind of information we can provide, but only if a specific order comes from the cabinet secretary's committee. But the UIDAI will never have any information on, say, whether a terrorist has bought a car... Even if the national security clause is invoked, we cannot get such information because we don't have it.

UNNI RAJEN SHANKER: Why is the UIDAI intolerant to any kind of criticism? There was an FIR against a reporter earlier this year.

I don't think we are intolerant. For filing an FIR there have to be two elements — violation of a law and criminal intent. If there is criminal intent, coupled with violation of law, then we feel duty bound to file an FIR. If we don't, then tomorrow we can be hauled up.

PRANAV MUKUL: Is the UIDAI open to ethical hackers and independent consultants?

This is a national identity system and has to be handled in a very responsible, mature and professional manner. Let's say someone has a system and they invite people to take a look at their system. Now let's say that person gets a small bit of information (the first time they access the system). In the next interaction, he gets another bit of information. In the next few days, he will know your weak points and how to attack you. Whenever we open up to the outside world, we have to be aware that we also have a responsibility. We should not take steps which we regret in hindsight. We have a strong multi-layer review mechanism to figure out whether we are doing something incorrect. We don't discuss many things in the public domain, particularly matters related to security.

MONOJIT MAJUMDAR: The Attorney General told the Supreme Court that the Aadhaar data is secure because it is hiding behind a '13-foot-high and 5-foot-wide wall'.

There was a context to it. The AG was giving an explanation to one of the petitioners who claimed that all the data is lying somewhere abroad. So, the AG, just to give an example to the court, said that the data centre is right here and very much protected. But it got reported differently in some sections of the media.

SUNIL JAIN: If there is a fear about how secure the Aadhaar data is, why don't you invite people to hack into the system and test it?

How do you know we haven't? As far as organising a 'hackathon' is concerned, there are many things that we do at our level — through the involvement of various agencies — but we can't put that in the public domain. This concerns sensitive data of 120 crore people... What we do to ensure security, if I start discussing it, then it can have other security implications. That is the balance that I have to strike. Normally, in any security exercise, if I have to disclose that this is the agency which did it, then people would know that these are the existing vulnerabilities which may be present later as well.

We are very serious about the security of data and take all the required steps... We are conscious of our responsibility at the UIDAI. In the past seven years, it's not that people did not try it (hacking). But we have thwarted all kind of attacks from both inside and outside the country and we have been able to keep the data safe. However, we can't boast about it and say my data is 100% safe. No technology expert can say that their data is 100% secure. I can only say that it was secure till yesterday. Security threats are changing so we need to constantly update our technology.