INTERVIEWS

'Centre & UIDAI are immune from prosecution over data leaks and breaches': cybersecurity expert

(/author/185891)

DHAIRYA MAHESHWARI
(/AUTHOR/185891)

Published: Jan 11th 2018, 06.17 PM

and-uidai-are-immune-from-prosecution-over-data-leaks-and-breaches-cybersecurity-expert&t=Without
on happening, says cybersecurity expert Pavan Duggal)

e-immune-from-prosecution-over-data-leaks-and-breaches-cybersecurity-
%20data%20leaks%20and%20breaches%E2%80%99%3A%20cybersecurity%20expert%C2%A0%20%C2%A0)

immune-from-prosecution-over-data-leaks-and-breaches-cybersecurity-expert)

ntre-and-uidai-are-immune-from-prosecution-over-data-leaks-and-breaches-cybersecurity-expert)

om-prosecution-over-data-leaks-and-breaches-cybersecurity-expert)

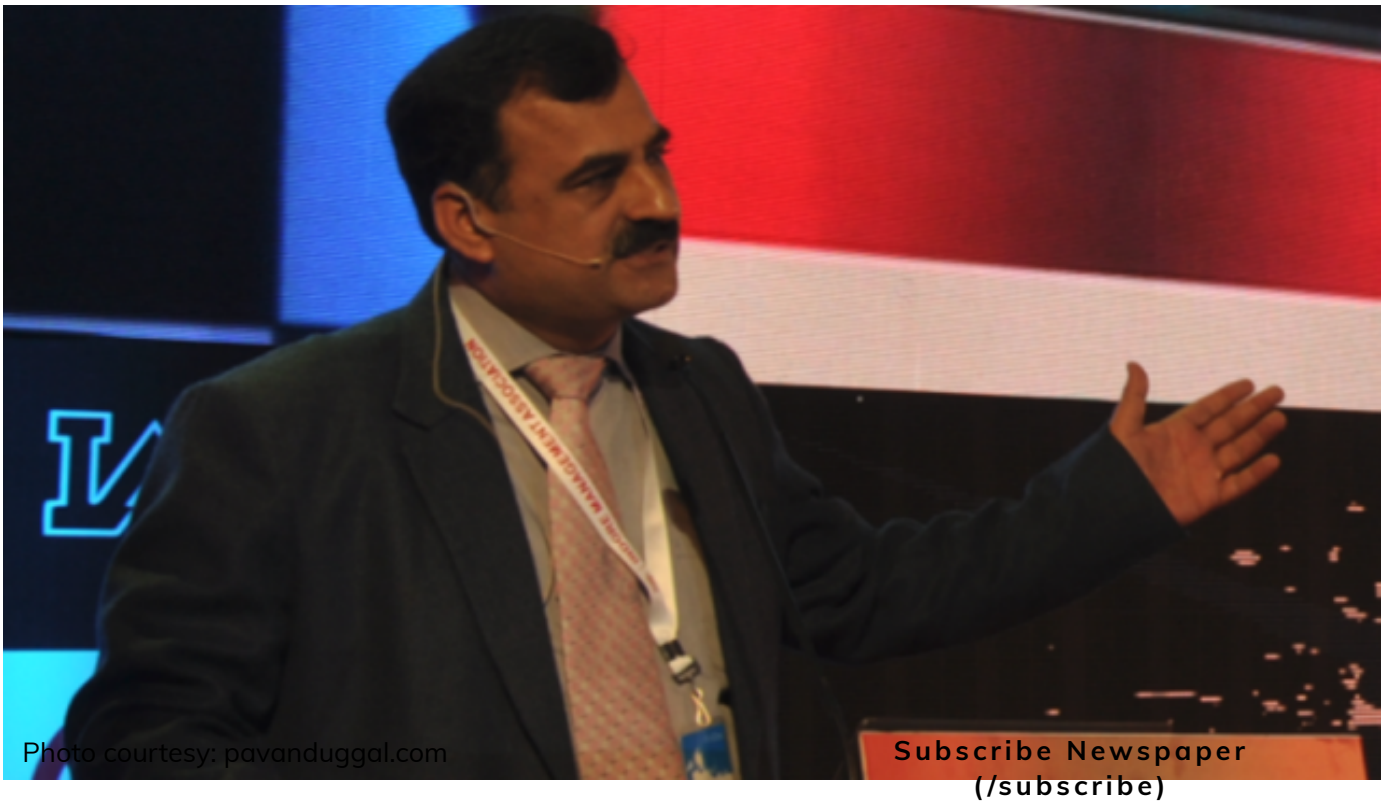


Photo courtesy: pavanduggal.com

File photo of cybersecurity expert Pavan Duggal

"Such a massive database has never been created anywhere else in the world previously. So, Aadhaar in a way is a foregone reality. Trying to retract it now will be a huge loss of face for govt."

For ₹500, anyone can access the Aadhaar database carrying biometric details of 1.19 billion Indians. Worse, anyone can forge anyone's identity on Aadhaar for an additional ₹300. A recent article in *The Tribune* highlighted some of the biggest flaws in the Aadhaar project, amid the Modi government's push to make it mandatory.

Without effective cybersecurity measures in place, such data breaches and instances of unauthorised access to Centre's databases would keep on happening, says cybersecurity expert Pavan Duggal. A Supreme Court lawyer, Duggal has been a vocal critic of Aadhaar since the project was launched in 2009, owing to concerns around national security and sovereignty.

Amid reports of Aadhaar data breaches and leaks, unauthorized accesses and impersonation among others, Duggal spoke to *National Herald*.

Edited excerpts:

How effective will the introduction of virtual IDs be in combating Aadhaar data breaches?

Introducing virtual identities appears to be a attractive concept, except the details of its technicalities and cyber security parameters are not fully visible in the circular. Further, the timing at which this so-called virtual identity concept is being sought to be introduced by June 1, 2018, is a suspect. It is like a person whose body has been exposed to radiation is post-radiation exposure given a shirt to wear, thinking that a shirt will help protect the body. But then the exposure has already taken place.

This virtual identity concept, first and foremost, is a voluntary concept. They have not made it mandatory. You are trying to create two set of classes in the Aadhaar ecosystem. One, of those people who are comfortable with virtually negligible levels of security and the other ones who may be more sensitive to their privacy and security. So, there are going to be huge practical challenges as we go forward in now implementing this midstream.

There are other practical challenges as well. First and foremost, the notification has been issued under the Aadhaar Act, 2016. It further seeks to introduce a concept which goes beyond the ambit and parameters of the Aadhaar Act. The circular

doesn't even stipulate as to under what sections has it been issued.

The UIDAI has been given the power to come up with various directions under Section 53 of Aadhaar Act. But the circular doesn't amount to a rule. Under Section 54 of Aadhaar Act, the UIDAI can introduce regulations. But this is also not a regulation. Obviously, regulations are made with the intention of carrying out the provisions of the Act. It goes a level below the regulation, as per the Aadhaar Act.

Further, the said circular runs contra to the provisions of the Act. Because under the Aadhaar Act, the government specified

A perusal of the Aadhaar Act shows that the Parliament never envisaged any concept of a virtual identity whatsoever. Now, introducing such a concept tantamounts to fundamentally changing the basis of Aadhaar. Therefore, this circular is likely to be potentially challenged in the court, inter alia among others, on the ground that the circular goes beyond the ambit of the Aadhaar Act.

Authentication of Aadhaar numbers can only be done under Section 8 of the Aadhaar Act. As per the legislation, introducing virtual identities in lieu of Aadhaar numbers is not permissible. The UIDAI cannot overreach the provisions of the Aadhaar Act through the circular. Aadhaar users also have this option of not sharing their Aadhaar numbers. But when I look at the detailed provisions as to how this exercise would be carried out, I don't see any cybersecurity measures being applied, which otherwise should have been an integral part of the architecture.

How will virtual identities end up protecting the data privacy as well as personal details of a person are things that aren't clear yet.

The way this artificial distinction is being sought to be made between Global AUAs and Local AUAs clearly shows at attempt to overreach the provisions of the law. The basic objective of the Aadhaar Act is to ensure that Aadhaar information is not leaked. But this exercise proposes that Global AUAs be able to store Aadhaar numbers on their systems. The devil will be in the details. The 16 paragraphs of the circular don't spell out the technical architecture by means of which these virtual identities will be generated, maintained, retained and persevered in a manner that is completely secure. A large number of people have unauthorized access to the Aadhaar database, making it possible for them to use Aadhaar numbers to generate fabricated or forged virtual IDs.

We now have 1.19 billion people on Aadhaar, which is the central reality. The government should come up with cogent solutions to make it more secure rather than coming up with paper notifications.

Indians should not be treated as experimental materials in the laboratories of the government. Already, Aadhaar Act has its own defects. If someone's Aadhaar number is compromised, they do not even have the power to go to police station and file an FIR. The circular is more like trying to repair a leaking roof with a Band-Aid. There has to be a more holistic, comprehensive and innovative approach that has to be followed.

The UIDAI has proposed the introduction of Global and private AUAs as part of the plan to bring in virtual Ids. Could you throw some light on these proposals?

The circular talks about AUAs in paragraph 9. This is a categorisation that they are seeking to make.

It is not also clear as to who all could be global and local AUAs. It is also not clear if these global AUAs will be located outside India, or if they would be Indian entities running operations from overseas. Similarly, local AUAs haven't been properly defined, but it may refer to domestic AUAs. Having said that, there is no basis in posing more confidence in AUAs by allowing them to store Aadhaar numbers. The categorization of AUAs again runs contrary to the natural principal of law as local AUAs won't have the power to store Aadhaar numbers.

So, the technical details are awaited by the UIDAI and how they plan to implement the proposal. The ground reality in implementation is very different from the broad motherly statements made in this circular. This circular won't transform itself into real implementation.

The Tribune **recently reported about the leak and sale of Aadhaar data by a private player. How dangerous are incidents like these and how could they be possibly prevented?**

The Tribune case points to very pertinent issues. It is the biggest flaw in the whole Aadhaar project that has come to fore since Aadhaar details got leaked in March 2016. Prior to this case, we were seeing various cybersecurity breaches, but the level of exposure was relatively related. We had 4.4 lakh Aadhar numbers leaked out from a Jharkhand government website. We had Aadhar information of more than 100 million people leaked during the Jio Aadhaar leaks.

But the Tribune report highlighted how access to the entire Aadhaar database was available for just ₹500. On top, any person's Aadhaar could be printed just for an additional payment of ₹300. The report just helped in reinforcing the point that Aadhaar is not safe.

Actually, Aadhaar has been suffering, thanks to the changing stands of the government. When it started out in 2009, it was a beta project. It started getting a push because many people started to think that having an Aadhaar number could be a form of strong governmental recognition.

Even when Aadhaar was legalised in 2016, it was still voluntary. So, the law only looked at the security of the data repositories storing all the biometric and geographic information. But then, the government started shifting its directions. It started making Aadhar mandatory. So, different services started getting connected to Aadhaar- bank accounts, income tax, company registrations and so on. Without anybody realising, an ecosystem started developing around Aadhaar. And this ecosystem is entirely unsafe. There are no parameters of cybersecurity. The stakeholders in this ecosystem have been storing people's Aadhaar numbers at will, because there was no regulation. Introducing virtual ID numbers is such an ecosystem is going to present many challenges. More significantly, any attack on Aadhaar could undermine national integrity, sovereignty and the security of the country. With biometrics of 1.19 billion people on it, Aadhaar has become India's critical information infrastructure.

Do you think that Aadhaar that had been envisaged at the time of United Progressive Alliance (UPA) in 2009 different from where the project is headed now? / Do you think the introduction of Aadhar was in a hurry and without having a full proof system?

From the word go, Aadhaar, as a project, was always a flawed exercise. What didn't seem to have been given adequate thought is that if you possess biometric details of 1.19 billion people, it is as if you are sitting on top of a live time bomb. Unless you could have had well thought out legal and regulatory strategies to protect and preserve biometric details, there were always going to be massive challenges.

The intrinsic problems of cyber security in Aadhaar were always there. For instance, the enrolment process for Aadhaar was done by sub contractors of often questionable credentials. Aadhaar numbers have bee given to dead persons, stones and trees. The authenticity and the veracity of this database are in question. Privacy was a concern but a big one as Aadhaar was optional.

But the moment the government started to make it mandatory, that's when privacy concerns started surfacing in public. While the repeated data breaches pointed to the fact that Aadhaar database wasn't secure enough, the authorities took an ostrich-in-the-sand approach as they gave out reassurances.

So, the work that should have gone into UIDAI had been missing. Now, it has evolved in such a huge monster that you don't know how to control it. Also, this practice was changing courses midway may prove counter-productive as it may create confusion leading to increased legal challenges for the government.

Is it possible now to junk the Aadhaar project?

Well, we have to wait for what the Supreme Court has to say during their judgment on privacy. If the SC thinks that Aadhaar is violative of privacy, it would state so.

However, from a pragmatic point of view, the government already has biometric information of 1.19 billion Indians. Such a massive database has never been created anywhere else in the world previously. So, Aadhaar in a way is a foregone reality. Trying to retract the project now will be a huge loss of face for the government. Aadhaar should have been reviewed long ago. The United Kingdom attempted a similar enterprise but halted it midway realising that such an exercise wouldn't be safe.

We must now try to identify the cybersecurity and privacy loopholes in the Aadhaar ecosystem and make it safer. Efforts should be made to strengthen Aadhaar.

Either to junk it or not is a decision that the government or the Supreme Court could make.

Was it a failure on part of the UIDAI to not have been able to ensure the security of Aadhar data and do the data breaches warrant FIRs against the UIDAI? Can the whistleblower who highlights data breaches be prosecuted under the law?

The UIDAI is exempt from any liability, by virtue of Section 52 of the Aadhaar Act, wherein the UIDAI and all its employees, along with Centre, cannot be prosecuted if the whatever they have carried out is in 'good faith'. Therefore, the government or the UIDAI can't be sued over the data breaches.

As for the whistleblowers, the Aadhar Act was never envisaged with the purpose of targetting journalists, or shooting the messenger. The penalties mentioned in Section 7 of the Act pertain to impersonation at the time of enrolment, unauthorised access to

the data repository and tampering with data with the central government among others. Broadly speaking, the Act aimed to protect the veracity and authenticity of the information of citizens, and not target any one pointing loopholes in the project.

The authorities have to be far more judicious in their use of law to target whistleblowers.

The Supreme Court would hear multiple petitions challenging Centre's decision to make Aadhaar mandatory. Do you think that is legally tenable?

Given the fact that the government's circular on virtual IDs talks of the move being introduced on June 1, the government is likely to seek an extension during the next hearing on March 31.

From a holistic viewpoint, we already have 1.19 billion people on Aadhaar. We should be very circumspect in making it mandatory without addressing cybersecurity concerns. There should be reasonable security in place as per the Information Technology Intermediary Rules, 2011. The Act says that power lies with the authorities, but there hasn't been enough information that's been propagated to public about cybersecurity measures in place.

Even the first circular of 2018 on virtual IDs remains silent on the details of how they will be protected and preserved by the AUAs. The Aadhar Act, 2016, must also be amended as it doesn't represent the changed ground realities. Remedies have to be given to persons whose Aadhar details have been compromised.

For all the latest India News, Follow India (https://www.nationalheraldindia.com/section/india) **Section.**

Aadhaar (/tag/aadhaar) UIDAI (/tag/uidai) Modi government (/tag/modi-government) national security (/tag/national-security) cybersecurity (/tag/cybersecurity) Pavan Duggal (/tag/pavan-duggal) virtual identity (/tag/virtual-identity)

ınd-uidai-are-immune-from-prosecution-over-data-leaks-and-breaches-cybersecurity-expert&t=Without
on happening, says cybersecurity expert Pavan Duggal)

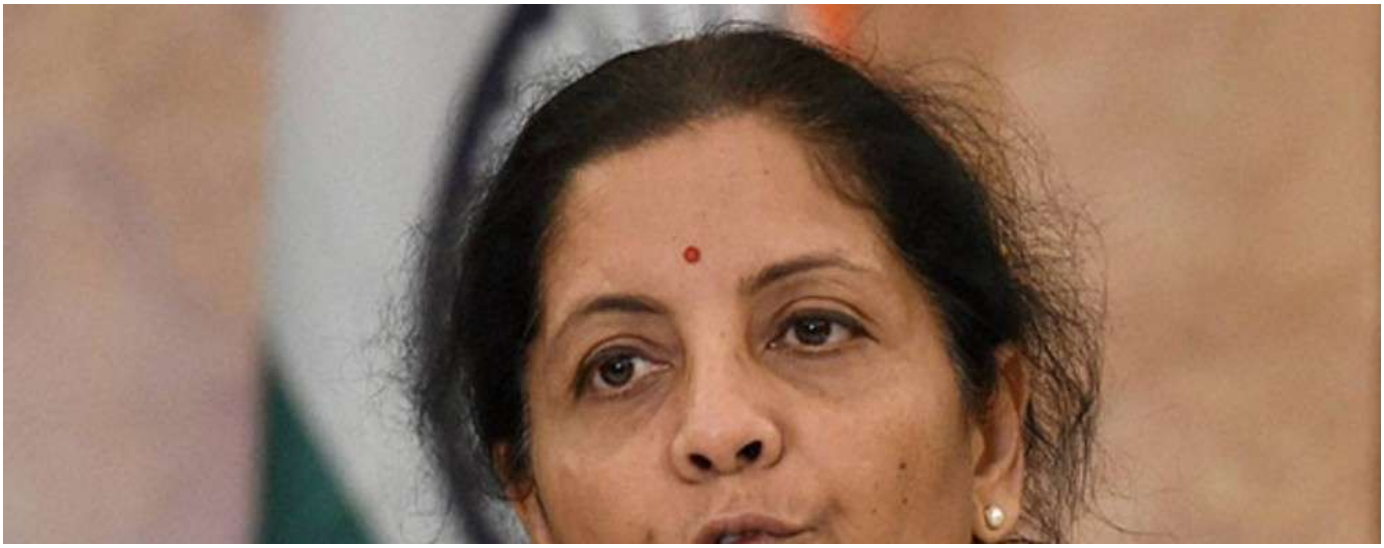
e-immune-from-prosecution-over-data-leaks-and-breaches-cybersecurity-
%20data%20leaks%20and%20breaches%E2%80%99%3A%20cybersecurity%20expert%C2%A0%20%C2%A0)

immune-from-prosecution-over-data-leaks-and-breaches-cybersecurity-expert)

ntre-and-uidai-are-immune-from-prosecution-over-data-leaks-and-breaches-cybersecurity-expert)

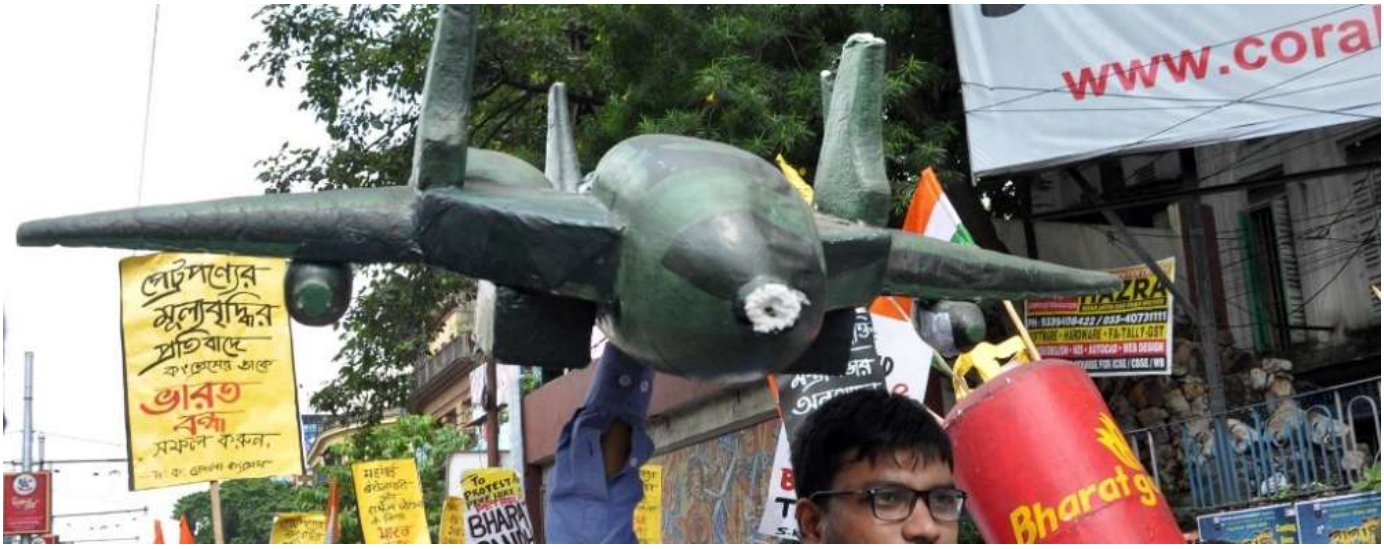
)m-prosecution-over-data-leaks-and-breaches-cybersecurity-expert)

MOST POPULAR



Nirmala Sitharaman at war with HAL, which comes under her own ministry

NITYA CHAKRABORTY/IPA | Sep 21st 2018, 07.00 AM
(/opinion/defence-minister-nirmala-sitharaman-is-at-war-with-her-own-ministry-departmental-undertaking-hal)



Govt sources say ex-HAL chief's claims on Rafale deal "factually incorrect"

IANS | Sep 21st 2018, 10.28 AM
(/national/central-government-sources-say-ex-hal-chief-ts-raju-claims-on-rafale-deal-factually-incorrect)

BACK TO TOP