# Numbers of security: UID case file

By Sunil Abraham, sunil@cis-india.org
Executive Director, Centre for Internet and Society

**Zero.** The probability of some evil actor breaking into the central store of authentication factors (such as keys and passwords) for the Internet. Why? That is because no such store exists. And the probability of someone evil breaking into the CIDR of the UIDAI? Greater than zero. How do we know? One, the central store exists and two, the Aadhaar Act lists breaking into this central store as an offence. Needless to say it would redundant to have a law that criminalises a technological impossibility. What is the consequence of someone breaking into the central store? Remember, biometrics is just a fancy word for non-consensual and covert identification technology. High resolution cameras can capture finger-prints and iris information from a distance. In other words, on the 16th of March 2016, when they passed the Act it was as if Indian law-makers wrote an open letter to criminals and foreign states saying "we are going to collect data to non-consensually identify all Indians and we are going to store it in a central repository. Come and get it!". Once again, how do I know that the CIDR will be compromised at some date in the future? How can I make that policy prediction with no evidence to back it up? To quote Sherlock Holmes "Once you eliminate the impossible, whatever remains, no matter how improbable, must be the truth." If a back door to the CIDR exists for the government then the very same back door could be used by an enemy within or from outside. In other words, the principle of decentralisation in cyber security does not require repeated experimental confirmation across markets and technologies.

**Zero.** The chances that you can fix through the law what you have broken through poor technological choices and architecture. And to a large extent vice versa. Aadhaar is a surveillance project masquerading as a development intervention because it uses biometrics. There is a big different between the government identifying you and you identifying yourself to the government. Let me say that again. Before UID, it was much more difficult for the government to identify you without your knowledge and without your conscious cooperation. Tomorrow, using high-resolution cameras and the power of big data – the government will be able to remotely identify those participating in a public protest. There will be no more anonymity in the crowd. I am not saying that law enforcement agencies and intelligence agencies should not use these powerful technologies to protect national security, uphold rule of law and protect individual rights. I am only saying that this type of surveillance technology is inappropriate for everyday interactions between the citizen and the state. Some software engineers believe that there are technical fixes for these concerns – they point to the consent layer in the India stack developed through a public-private partnership with the UIDAI. But this is exactly what Evgeny Morozov has dubbed "technological solutionism" - fundamental flaws like this cannot be fixed by legal or technical band aid. If you were to ask the UIDAI – how do you ensure that the data does not get stolen between the enrollment machine and the CIDR – they respond saying – we use state of the art cryptography. If cryptography is good enough for UIDAI – why is it not good enough for citizens? That is because if citizens use cryptography [on smart cards] to identify themselves to the state – the state will need their conscious cooperation each time. That provides the feature that is required for better governance without the surveillance bonus. If you really must use biometrics – it could be stored on the smart card after being digital signed by the enrollment officer. If there is every a doubt whether the person has stolen the smart card – a special machine could be used to read the biometrics off the card and check against the person. This way the power of biometrics would be leveraged without any of the accompanying harms.

**Zero.** This time for the utility of biometrics as a password or authentication factor. There are two principle reasons for which the Act should have prohibited the use of biometrics for authentication.

First, biometric authentication factors are irrevocable unlike passwords, PINs, digital signatures etc. Once a biometric authentication factor has been compromised, there is no way to change it. The security of a system secured by biometrics is permanently compromised. Second, our biometrics are so easy to steal – we leave our finger prints everywhere. Also, if I upload my biometric data onto the Internet, I could then plausibly deny all transactions against my name in the CIDR. In order to prevent me from doing that - the government would have to invest in CCTV cameras [with large storage] as they do for passport control borders and as banks do at ATMs. If you are anyway having to invest in CCTV cameras then you might as well stick with digital signatures on smart cards as the previous NDA government had proposed the SCOSTA (Smart Card Operating System Standard for Transport Application) standard for the MNIC (Multipurpose National ID Card). Leveraging smart card standards like EMV will ensure harnessing greater network effects thanks to the global financial infrastructure of banks. These network effects will drive down cost of the equipment and afford Indians greater global mobility. And most importantly when a digital signature is compromised – the user can be issued a new smart card. As Rufo Guerreschi, Executive Director of Open Media Cluster puts it "world leaders, and IT experts should realize that citizen freedoms and states' ability to pursue suspects are not an 'either or' but a 'both or neither'."

**Near zero.** We now move the biometrics as the identification factor. The rate of potential duplicates or "False Positive Identification Rate" which according to the UIDAI is only 0.057%. Which according to them will result in only "570 resident enrollments will be falsely identified as duplicate for every one million enrollments." However, according to an article published in the Economic and Political Weekly by my colleague at the Centre for Internet and Society, Hans Verghese Mathews this will result in one out of every 146 people being rejected during enrollment when total enrollment reaches 1 billion people. In their rebuttal, the UIDAI dispute the conclusion but they offer no alternative extrapolation or mathematical assumptions. "Without getting too deep into the mathematics" they offer an account of "a manual adjudication process to rectify the biometric identification errors". This manual adjudication determines whether you exist and has none of the elements of natural justice such as notice to the affected party and opportunity to be heard. Elimination of ghosts is impossible if only machines and unaccountable humans perform this adjudication. This is because there is zero skin in the game. There are free tools available on the Internet such as **SFinGe** (**S**ynthetic **Fin**gerprint **Ge**nerator) which allow you to create fake biometrics. The USB cables on the UIDAI approved enrollment setup can be intercepted using generic hardware that can be bought online. With a little bit of clever programming countless number of ghosts can be created which will easily clear the manual adjudication process that UIDAI claims will ensure that "no one is denied an Aadhaar number because of a biometric false positive."

**Near zero.** This time for surveillance, which I believe should be used like salt in cooking. Essential in small quantities but counter productive even if slightly in excess. There is a popular misconception that privacy researchers such as myself are opposed to surveillance. In reality, I am all for surveillance. I am totally convinced that surveillance is good anti-corruption technology. But I also want good return on investment for my surveillance tax rupee. According to Julian Assange transparency requirements should be directly proportionate to power – in other words the powerful should be subject to more surveillance. And conversely I add, privacy protections must be inversely proportionate to power – or again in other words the poor should be spared from intrusions that don't serve the public interest. The UIDAI make the exact opposite design assumption – it assumes that the poor are responsible for corruption and that technology will elimintate small-ticket or retail corruption. But we all know that politicians and bureaucrats are responsible for most large-ticket corruption. Why doesn't the UIDAI first assign UID numbers to all politicians and bureaucrats? Then using digital signatures why don't we ensure that we have a public non-repudiable audit trail wherein everyone can track the follow of benefits, subsidies and services from New Delhi to the panchayat office or local corporation office? That would eliminate big-ticket or whole sale corruption. In other words, since most of Aadhaar's surveillance is targeted at the bottom of the

pyramid there will be limited bang for the buck. Sousveillance is the need of the hour - we need more CCTVs with microphones turned on in government offices than biometric devices in slums.

**One. And zero.** In the contemporary binary and digital age, we have lost faith in the old Gods. Science and its instantiation technology have become the new Gods. The cult of technology is intolerant to blasphemy for example Shekhar Gupta recently tweeted saying that part of the opposition to Aadhaar was because "left-libs detest science/tech." Technology as ideology is based on some fundamental articles of faith – one - new technology is better than old technology, two - expensive technology is better than cheap technology, three - complex technology is better than simple technology, and four - all technology is empowering or at the very least neutral. Unfortunately there is no basis in science for any of these articles of faith. Let me use a simple story to illustrate. I was fortunate to serve as a member of committee that Department of Biotechnology established to finalize the Human DNA Profiling Bill 2015 which was to be introduced in Parliament last monsoon. Aside: the language of the Act also has room for the database to expand into a national DNA database circumventing ten years of debate around the controversial DNA Profiling Bill 2015. The first version of this Bill that I read in January 2013 said DNA profiling is "powerful technology that makes it possible to determine whether the source of origin of one body substance is identical to that of another … without any doubt." In other words to quote K.P.C. Gandhi, scientist from Truth Labs, "I can vouch for the scientific infallibility of using DNA profiling for carrying out justice." Unfortunately though the infallible science is conducted by fallible humans. During one of the meetings a scientist described the process of generating a biometric profile. The first step after the lab technician generated the profile was to compare the generated profile with her or his own profile because during the process of loading the machine with the DNA sample some of the lab technician's DNA could have contaminated the sample. This error would not be a possibility in much older, cheaper and rudimentary biometric technology for ex. photography. A photographer developing a photograph in a dark room does not have to ensure that his or her own image has not accidentally ended up on the negative. But the UIDAI is filled with die-hard techno-utopians, if you tell them that finger prints won't work for those who are engaged in manual labour – they will say then we will use iris based biometrics. But again complex technologies are more fragile and often come with increased risks – they may provide greater performance and features but sometimes they are easier to circumvent. A gummy finger to fool a biometric scanner can be produced using Fevicol and a candle but to fake a passport takes a lot of sophisticated technology. Therefore it is important for us as a nation to give up our unquestioning faith in technology and start to debate exact technological configurations of surveillance technology for different contexts and purposes.

**One.** This time representing a monopoly. Prior to the UID project, nobody got paid when citizens identified themselves to the state. While the Act says that UIDAI will get paid – it does not specify how much. Sooner or later this cost of identification will be passed on to citizens and residents. There will be a consumer service provider relationship established between the citizen and the state when it comes to identification. The UIDAI will become the monopoly provider of identification and authentication services in India that is trusted by the government. That sounds like a centrally planned communist state to me. Shouldn't the right-wing oppose the Act because it prevents the free market from working? Shouldn't the free market pick the best technology and business model for identification and authentication? Won't that drive the cost of identification and authentication down and ensure higher quality of service for citizens and residents? Competing providers could also publish transparency reports regarding their compliance with data requests from law enforcement and intelligence agencies and if this is important is important to consumers they will be punished by the market. The government can use mechanisms like permanent and temporary bans and price regulation as disincentives for the creation of ghosts. There will be a clear financial incentive to keep the database clean. Just like the government established regulatory framework for digital certificates in the IT Act allowing for e-commerce and e-governance. Ideally the Aadhaar

Act should have done something similar and established a ecosystem for multiple actors to provide services in this two-sided market. For it is impossible for a "small government" to have the expertise and experience to run one of the world's largest database of biometric and transaction records securely for perpetuity.

To conclude - I support the use of biometrics. I support government use of identification and authentication technology. I support the use of ID numbers in government databases. I support targeted surveillance to reduce corruption and protect national security. But I believe all these must be put into place with care and thought so that we don't end up sacrificing our constitutional rights or compromising the security of our nation state. Unfortunately, the Aadhaar project's technological design and architecture is an unmitigated disaster and no amount of legal fixes in the Act will make it any better. Our children will pay a heavy price for our folly in the years to come. To quote security guru – Bruce Schneier "Data is a toxic asset. We need to start thinking about it as such, and treat it as we would any other source of toxicity. To do anything else is to risk our security and privacy."