5

Surveillance Project*

Sunil Abraham

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. The decentralised architecture of the internet means that there is no ‘single point of failure’. And, what is the probability of someone evil breaking into the Central Identities Data Repository (CIDR) of the Unique Identification Authority of India (UIDAI)? Greater than zero. How do we know this? One, the central store exists and two, the Aadhaar Act lists breaking into this central store as an offence. Needless to say, it would be 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—technology which empowers the state to identify you by measuring your body. Today this can be done from a distance, since high-resolution cameras can remotely capture fingerprints and iris information.

In other words, on 16 March 2016, when Parliament passed the Aadhaar Act, it was as if Indian lawmakers 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 backdoor to the CIDR exists for the government, then the very same backdoor can be used by an enemy within or from outside. As Bitcoin guru Andreas M. Antonopoulos has repeatedly reminded us, all centralised databases are honeypots, the question is not if they will be compromised but when they will be compromised. 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 with the law what you have broken with poor technological choices and architecture. And, to a large extent vice versa, you cannot use good technology to fix bad law. Aadhaar is a surveillance project masquerading as a development intervention because it uses biometrics. Globally informed consent is considered the foundation of privacy and data protection law. When a citizen uses Aadhaar, there is no way of verifying if there was consent since both authentication and identification for subsidies or services do not require the conscious cooperation of the data subject. Unless the citizen has a mobile phone, they will not even be notified of the transaction. There are a variety of ways in which corrupt officials can take advantage of this poor technological choice—they could say (a) the machine is not working; (b) the network is not working; or (c) the CIDR is not working, etc. even if the authentication has been successful. Aadhaar makes the citizen transparent to the state but makes the state completely opaque and unaccountable to its citizens.

There is a big difference between the government identifying you and you identifying yourself to the government. Before UID, it was much more difficult for the government to identify you without your knowledge and 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 ensure national security, uphold the 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. Since we started research on Aadhaar in 2010, we have been warning of the misuse of the surveillance potential of the Aadhaar project. Today, many who dismissed this view have had to change their minds.

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 do not get stolen between the enrolment machine and the CIDR, the response would be, ‘we use state-of-the-art cryptography’. If cryptography is good enough for the UIDAI, why is it not good enough for citizens? That is because if citizens use cryptography (for example, 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 digitally signed by the enrolment officer. If there is ever a doubt whether the person has stolen the smart card, a special machine can be used to read the biometrics off the card and check that against the person. This way, the power of biometrics would be leveraged without any of the associated harms to security, privacy, equality, inclusion and dignity.

Zero: this time, for the utility of biometrics as a password or authentication factor. There are two principal 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. Imagine not being able to change your lock after you know the key has been stolen. The security of a system secured by biometrics is permanently compromised. Second, our biometrics are impossible to secure and very easy to steal; for example, we leave our fingerprints on almost every surface we touch.

Also, if I upload my biometric data onto the internet, I can then plausibly deny all transactions against my name in the CIDR. In order to prevent me from doing that, the government will have to invest in CCTV cameras [with large storage] as they do for passport-control borders and as banks do at ATMs. If you anyway have to invest in CCTV cameras, then you might as well stick with digital signatures on smart cards, as the previous National Democratic Alliance (NDA) government proposed the SCOSTA (Smart Card Operating System Standard for Transport Application) standard for the MNIC (Multipurpose National ID Card). Leveraging proprietary smart card standards like EMV (Europay Visa Mastercard) or, better still, equivalent open standards, will ensure harnessing greater network effects thanks to the global financial infrastructure of banks. These network effects will drive down the cost of 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 realise that citizen freedoms and states' ability to pursue suspects are not an "either or" but a "both or neither".' Once a privacy-undermining mass surveillance system has been built, you cannot predict what use it will be put to by a future repressive government, a rogue corporation, criminals or terrorists. The chilling effects on the rights to free speech, association and assembly will be felt as soon as citizens understand the scale of the surveillance.

Near zero: We now move to biometrics as the identification factor. The rate of potential duplicates or 'False Positive Identification Rate' which, according to the UIDAI, is only 0.057 per cent. According to them, only '570 resident enrolments will be falsely identified as duplicate for every one million enrolments'. 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 (2016), this will result in one out of every 146 people being rejected during enrolment when total enrolment reaches 1 billion people. In its rebuttal, the UIDAI disputes the conclusion but offers no alternative extrapolation or mathematical assumptions. 'Without getting too deep into the mathematics', it offers 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 individuals and opportunity to be heard. The architecture of the system allows the government to shirk responsibility when rights are infringed and pass the blame on to an inscrutable black box. 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 (Synthetic Fingerprint Generator), which allow you to create fake biometrics. The USB cables on the UIDAI-approved enrolment setup can be intercepted using generic hardware that can be bought online. I predicted in 2011 that with a little bit of clever programming, countless number of ghosts can be created which will easily clear the manual adjudication process that the UIDAI claims will ensure that 'no one is denied an Aadhaar number because of a biometric false positive'. This prediction came true this year when the police arrested a gang of criminals that had created a ghost enrolment kit and were selling it along with silicon copies of fingerprints of enrolment officers almost as if they were running a franchise operation.

Near zero: this time for surveillance, which, I believe, should be used like salt in cooking—essential in small quantities, but counterproductive 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 returns 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—in other words, the poor should be spared from intrusions that do not serve the public interest. The UIDAI makes the exact opposite design assumption; it assumes that the poor are responsible for corruption and that technology will eliminate small-ticket or retail corruption. But we all know that the powerful (politicians and bureaucrats, for example) are responsible for most large-ticket corruption.

Why does not the UIDAI first assign UID numbers to all politicians and bureaucrats? Then using digital signatures, why do we not ensure that we have a public, non-repudiable audit trail wherein everyone can track the flow of benefits, subsidies and services from New Delhi to the panchayat office or local corporation office? That will eliminate big-ticket or wholesale 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. If surveillance 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 this. I was fortunate to serve as a member of a committee that the Department of Biotechnology established to finalise the Human DNA Profiling Bill, 2015, which was to be introduced in Parliament. Aside: the language of the Act also has room for the database to expand into a national DNA database, circumventing 10 years of debate around the controversial DNA Profiling Bill, 2015. The first version of this Bill that I read in January 2013 said that DNA profiling was a '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, a 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 laboratory 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 laboratory technician's DNA could have contaminated the sample. This error would not be a possibility in much older, cheaper and rudimentary biometric technology, for example, photography. A photographer developing a photograph in a darkroom does not have to ensure that his or her own image has not accidentally ended up on the negative. But the Aadhaar promoters are die-hard techno-utopians; if you tell them that fingerprints will not work for those who are engaged in manual labour, they recommend the use of 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 glue and a candle, but to fake a passport takes a lot of sophisticated technology. The data from the field show that even iris-based authentication has unacceptably high failure rates. Therefore, it is important for us to give up our unquestioning faith in technology and start to debate the 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. Now the UIDAI will get paid every time this happens and every time citizens wish to update their information in the CIDR. The cost of identification has been passed on to those being identified, we are paying to be surveilled. 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 which is trusted by the government. That sounds like a centrally planned communist state to me. Should not the right-wing oppose the Act because it prevents the free market from working? Should not the free market pick the best technology and business model for identification and authentication? Will not that drive the cost of identification and authentication down and ensure higher quality of service for citizens and residents?

Competing providers can also publish transparency reports regarding their compliance with data requests from law-enforcement and intelligence agencies, and if this is important to consumers, they will be punished by the market. The government can use mechanisms such as 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 a regulatory framework for digital certificates in the Information Technology Act, allowing for e-commerce and e-governance. Ideally, the Aadhaar Act should have done something similar and established an eco-system 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 databases 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 in place with care and thought so that we do not 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 the 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.'

Reference

Mathews, Hans Verghese. 2016. ‘Flaws in the UIDAI Process’. *Economic and Political Weekly* 51 (9), pp. 74–78.

∗ A previous version of this chapter was published as Sunil Abraham, 2016, ‘Surveillance Project’, *Frontline*, 15 April.