Who am I?

- 3rd Year
- Twitter: @Zack_Not_Zac
- Slack: zackattack
- GitHub: zack-not-zac

Zack

@Zack_Not_Zac

Current mood = the cat you see above. One of the @AbertayHackers

10 Fingerprints & 2 Iris Scans - Just To Pay For Electricity

The glaring issues with India’s identification system – and the recent trend of companies storing more and more user data.

What is Aadhaar?

- Ideally – a fool proof identification system that prevents fake I.D’s
- Reality – a mess

What is it for?

- Accessing government facilities
  - Paying Taxes
  - Welfare
  - Pensions
- Proof of identity (even though the government say it shouldn’t be) and residence
- Bank Accounts
- Phone Contracts
- Gas and Electricity
- Each I.D number is supplied by the Unique Identification Authority of India (UIDAI) and stored in a *single centralised data centre*.

Other Facts

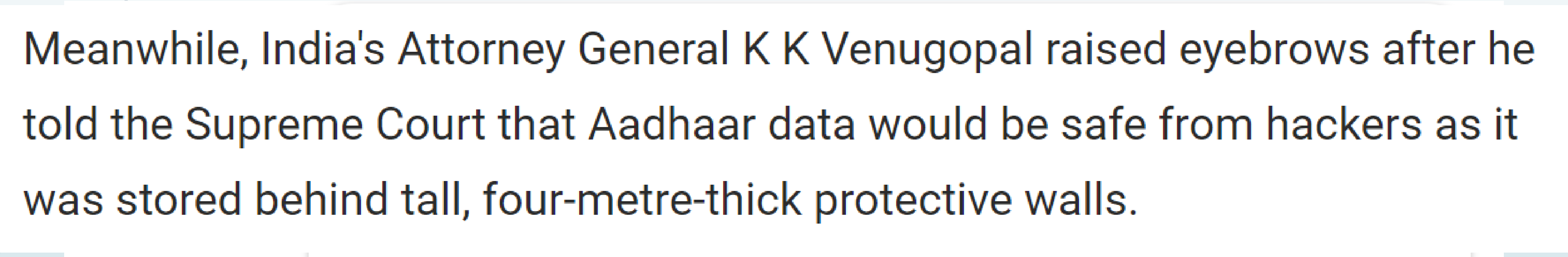
- 90% of total population (over 1.2 billion people) hold an Aadhaar number.
- More than 21 billion banking and other digital transactions take place annually under the scheme.

What’s the issue? (Its shit)

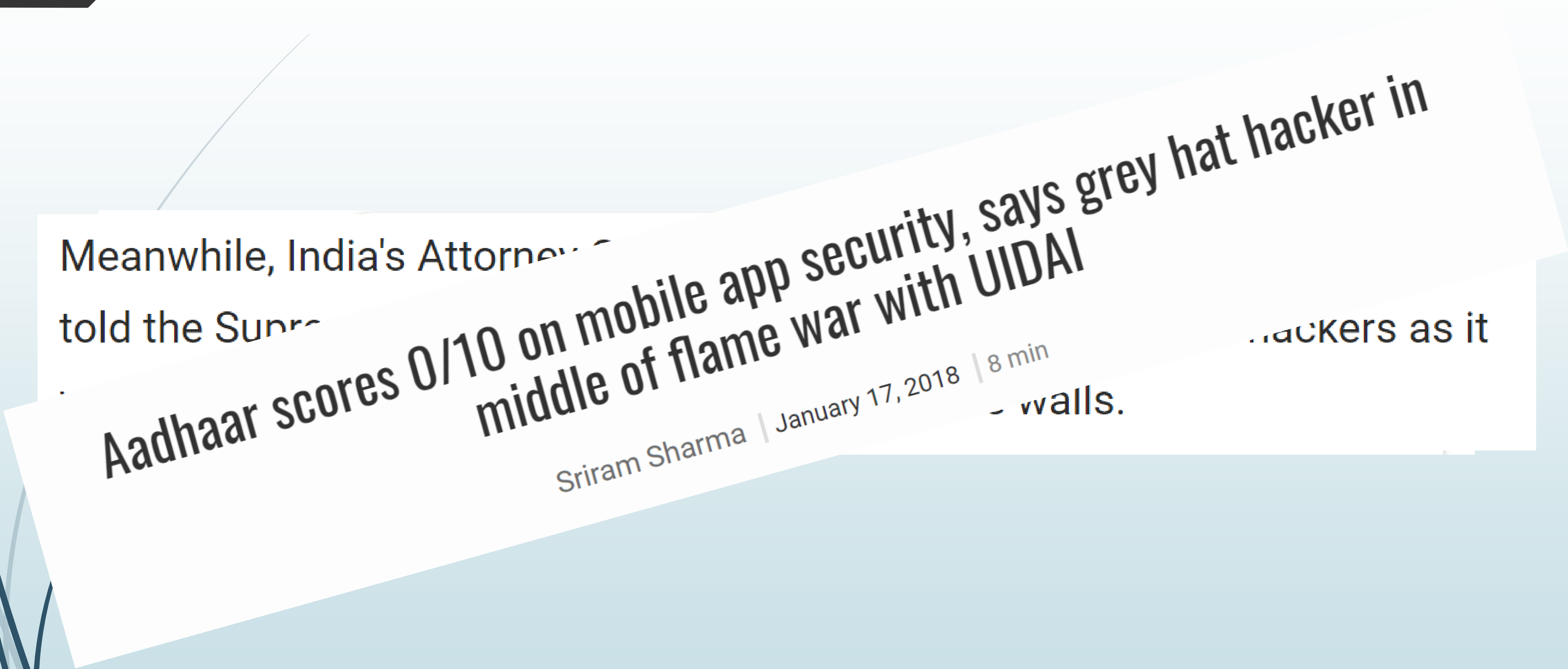
- Reliance on the scheme has made it almost compulsory (violating various rights to privacy in India)

- The Minister for Information Technology told local media that the biometric records in the Aadhaar data vault could not be hacked "even with the billionth effort."

- Even if the vault is “fairly secure”, the services and infrastructure that use it are not.



Meanwhile, India's Attorney General K K Venugopal raised eyebrows after he told the Supreme Court that Aadhaar data would be safe from hackers as it was stored behind tall, four-metre-thick protective walls.



Aadhaar scores 0/10 on mobile app security, says grey hat hacker in middle of flame war with UIDAI

Sriram Sharma | January 17, 2018 | 8 min

Meanwhile, India's Attorney

told the Supr

ackers as it

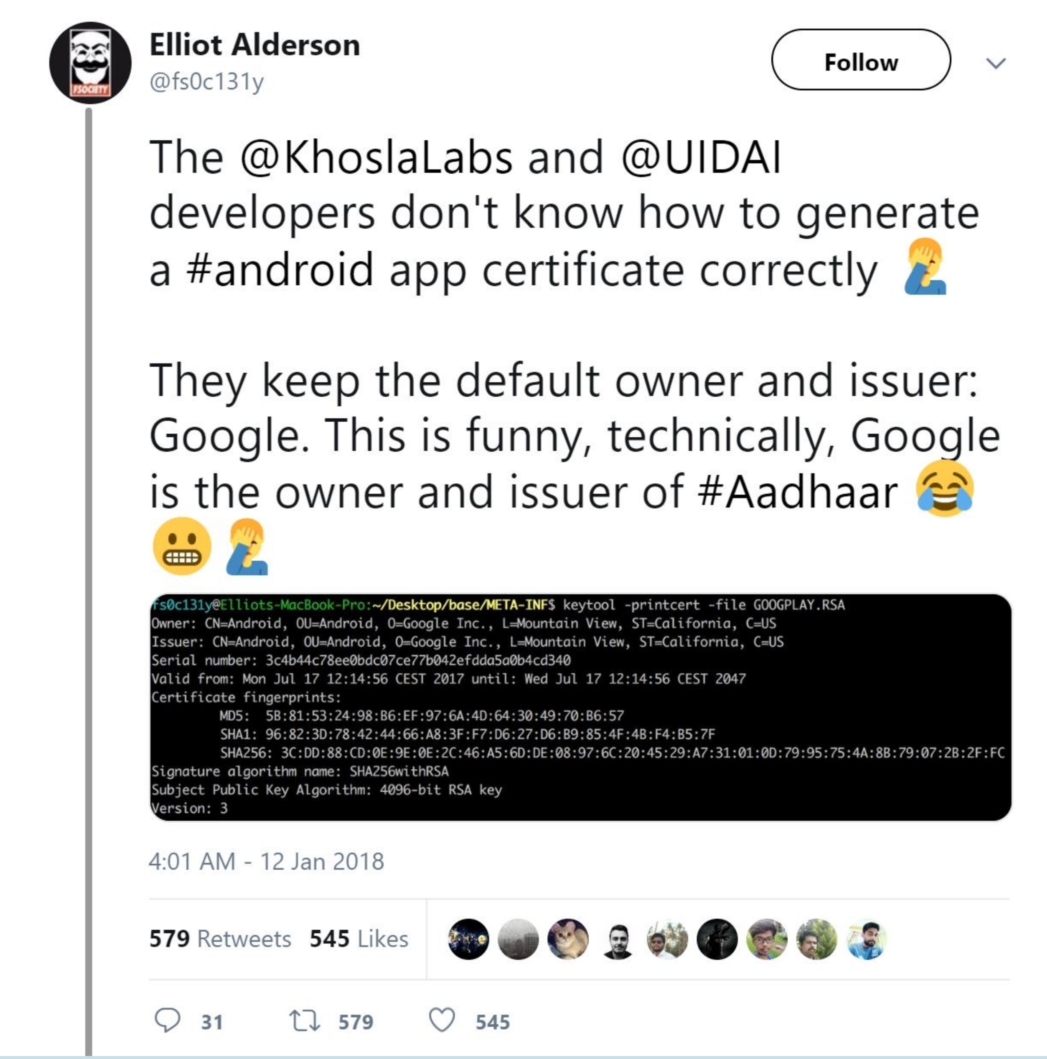
walls.

The App

- Baptiste Robert (Also known as @fs0c131y) decompiled the Android App
  - Extracted the database password and password salt
    - Concluded it was the same for every user.
- They don’t know how to generate certificates.

The App

- Bapti piled the Android App
  - Ex
- They



Elliot Alderson
@fs0c131y

The @KhoslaLabs and @UIDAI developers don't know how to generate a #android app certificate correctly 🤦‍♂️

They keep the default owner and issuer: Google. This is funny, technically, Google is the owner and issuer of #Aadhaar 😂 😬 🤦‍♂️

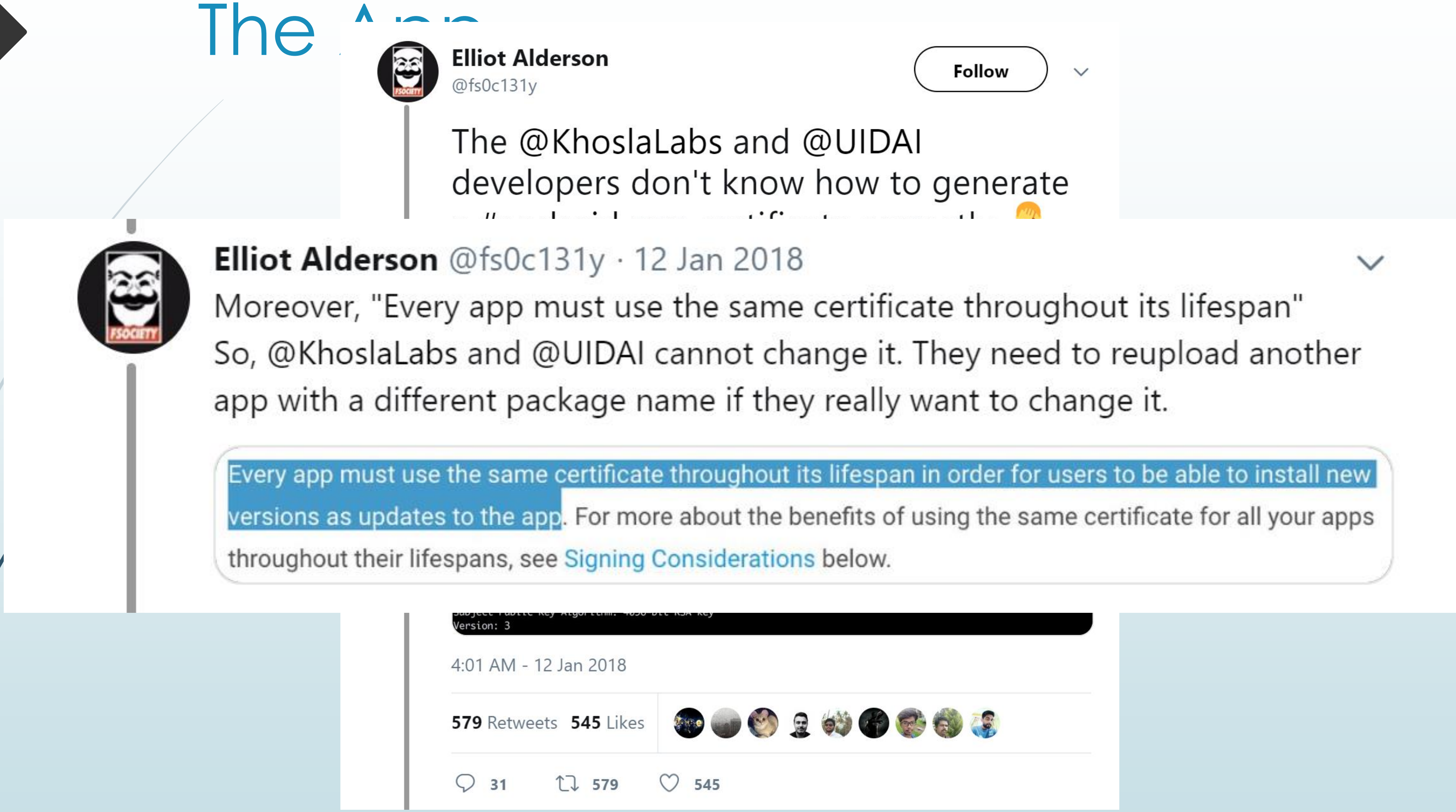
```
fs0c131y@Elliots-MacBook-Pro:~/Desktop/base/META-INF$ keytool -printcert -file GOOGPLAY.RSA
Owner: CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=California, C=US
Issuer: CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=California, C=US
Serial number: 3c4b44c78ee0bdc07ce77b042efdda5a0b4cd340
Valid from: Mon Jul 17 12:14:56 CEST 2017 until: Wed Jul 17 12:14:56 CEST 2047
Certificate fingerprints:
         MD5:  5B:81:53:24:98:B6:EF:97:6A:4D:64:30:49:70:B6:57
         SHA1: 96:82:3D:78:42:44:66:A8:3F:F7:D6:27:D6:B9:85:4F:4B:F4:B5:7F
         SHA256: 3C:DD:88:CD:0E:9E:0E:2C:46:A5:6D:DE:08:97:6C:20:45:29:A7:31:01:0D:79:95:75:4A:8B:79:07:2B:2F:FC
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
```

4:01 AM - 12 Jan 2018

579 Retweets 545 Likes

The App

pp



Elliot Alderson
@fs0c131y

Follow

The @KhoslaLabs and @UIDAI developers don't know how to generate

Elliot Alderson @fs0c131y · 12 Jan 2018

Moreover, "Every app must use the same certificate throughout its lifespan"
So, @KhoslaLabs and @UIDAI cannot change it. They need to reupload another app with a different package name if they really want to change it.

Every app must use the same certificate throughout its lifespan in order for users to be able to install new versions as updates to the app. For more about the benefits of using the same certificate for all your apps throughout their lifespans, see Signing Considerations below.

```
Version: 3
```

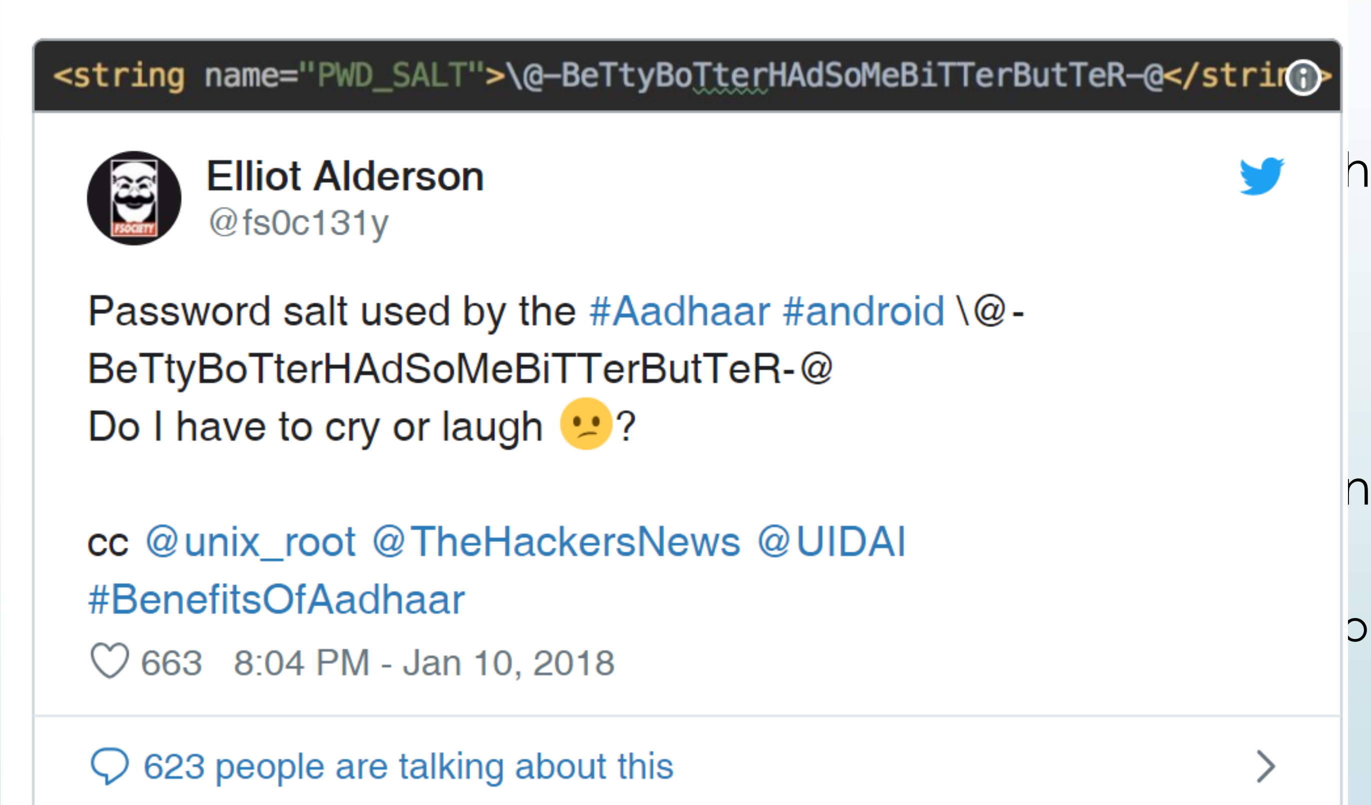
4:01 AM - 12 Jan 2018

579 Retweets 545 Likes

The App

- Baptiste Robert (Also known as @fs0c131y) decompiled the Android App
  - Extracted the local database password and password salt
    - Concluded it was the same for every user.
- They don't know how to generate certificates.
- Jump straight to creating a new password with no authentication: https://twitter.com/fs0c131y/status/953184798838853632
  - Would require Android Debugging to be enabled and authorised, as well as physical access to the device.

The App



```
<string name="PWD_SALT">\@—BeTtyBoTterHAdSoMeBiTTerButTeR—@</strin
```

Elliot Alderson
@fs0c131y

Password salt used by the #Aadhaar #android \@-BeTtyBoTterHAdSoMeBiTTerButTeR-@
Do I have to cry or laugh 😕?

cc @unix_root @TheHackersNews @UIDAI #BenefitsOfAadhaar

♡ 663 8:04 PM - Jan 10, 2018

623 people are talking about this

- he Android App
- ntication:
  orised, as well as

The App

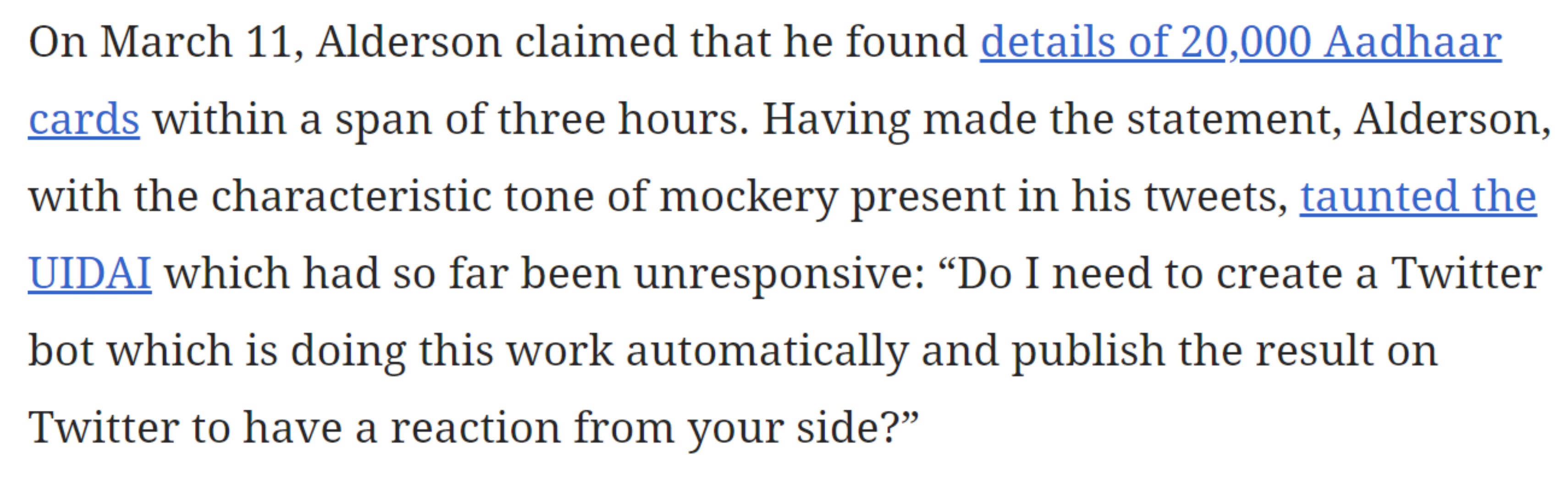
- Baptiste Robert (Also known as @fs0c131y) decompiled the Android App
  - Extracted the local database password and password salt
    - Concluded it was the same for every user.
- They don't know how to generate certificates.
- Jump straight to creating a new password with no authentication: https://twitter.com/fs0c131y/status/953184798838853632
  - Would require Android Debugging to be enabled and authorised, as well as physical access to the device.

Leaks

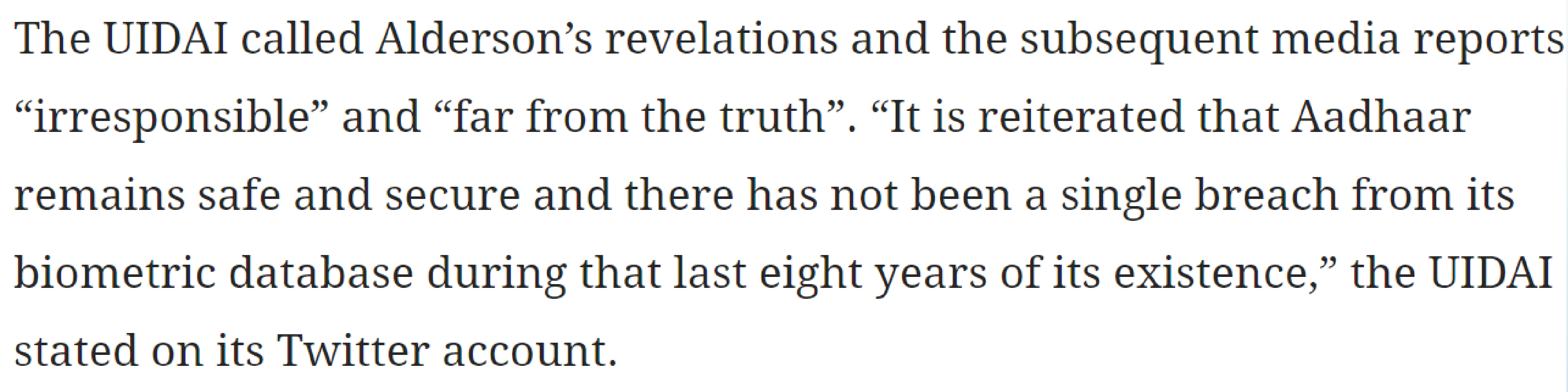
- In January 2018 it was exposed that anonymous WhatsApp users were offering services for 500 rupees (about £5.80) which gave the client an administrator login to the database and view all personal details about a user – excluding biometrics.
- For an extra 300 rupees, they'd also throw in a piece of software that allowed the client to print any card they wanted.

AND REPAIRED IT WITH
ONLY FLEX TAPE
FLEX TAPE

More Leaks



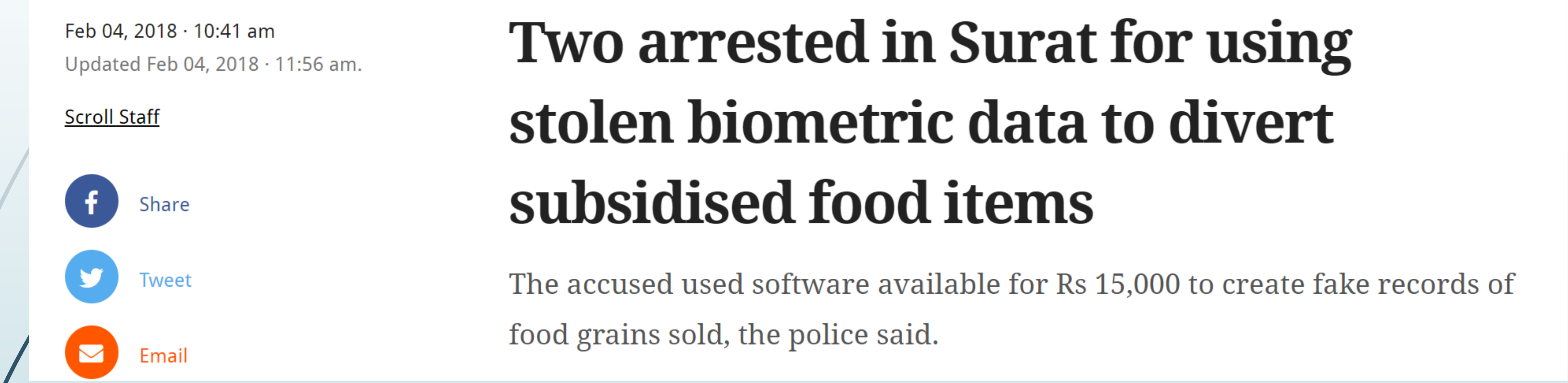
On March 11, Alderson claimed that he found details of 20,000 Aadhaar cards within a span of three hours. Having made the statement, Alderson, with the characteristic tone of mockery present in his tweets, taunted the UIDAI which had so far been unresponsive: “Do I need to create a Twitter bot which is doing this work automatically and publish the result on Twitter to have a reaction from your side?”



The UIDAI called Alderson’s revelations and the subsequent media reports “irresponsible” and “far from the truth”. “It is reiterated that Aadhaar remains safe and secure and there has not been a single breach from its biometric database during that last eight years of its existence,” the UIDAI stated on its Twitter account.

LEFT
EXIT 12
I can access your data
"Not a single breach in our Biometrics database"

No Breach != No Leak



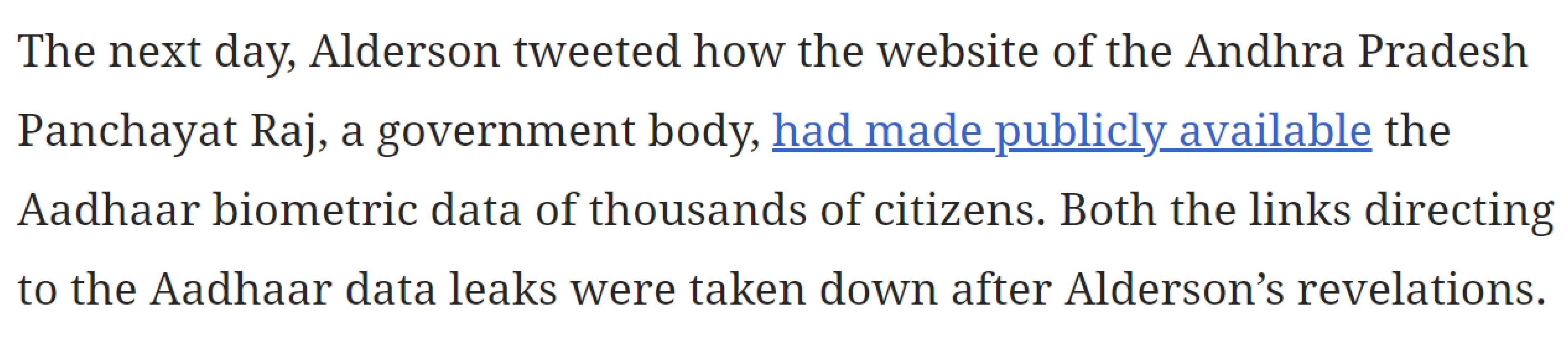
Feb 04, 2018 · 10:41 am
Updated Feb 04, 2018 · 11:56 am.

Scroll Staff

Two arrested in Surat for using stolen biometric data to divert subsidised food items

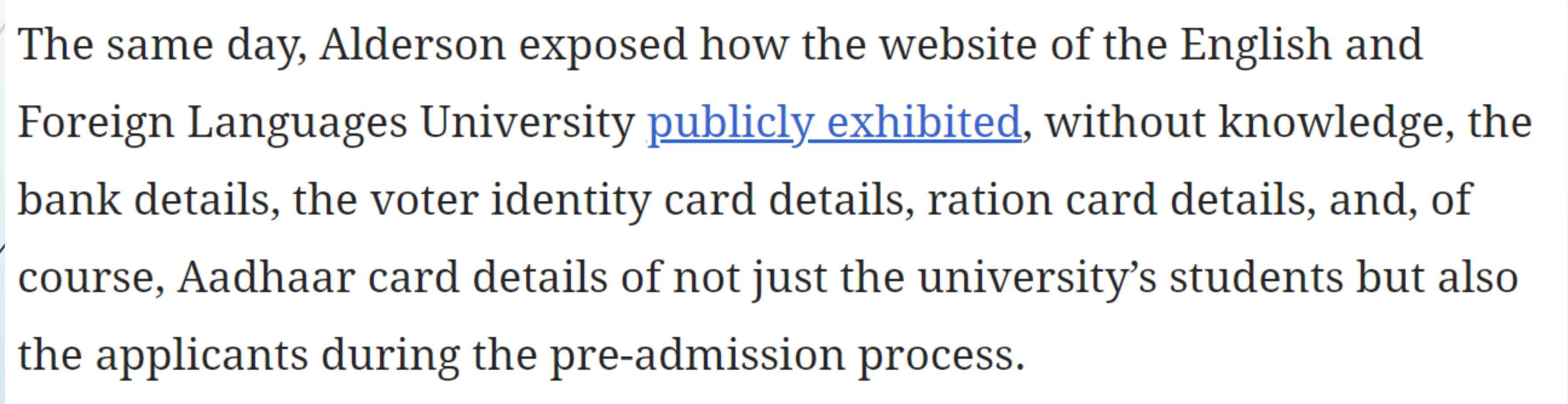
The accused used software available for Rs 15,000 to create fake records of food grains sold, the police said.

No Breach != No Leak



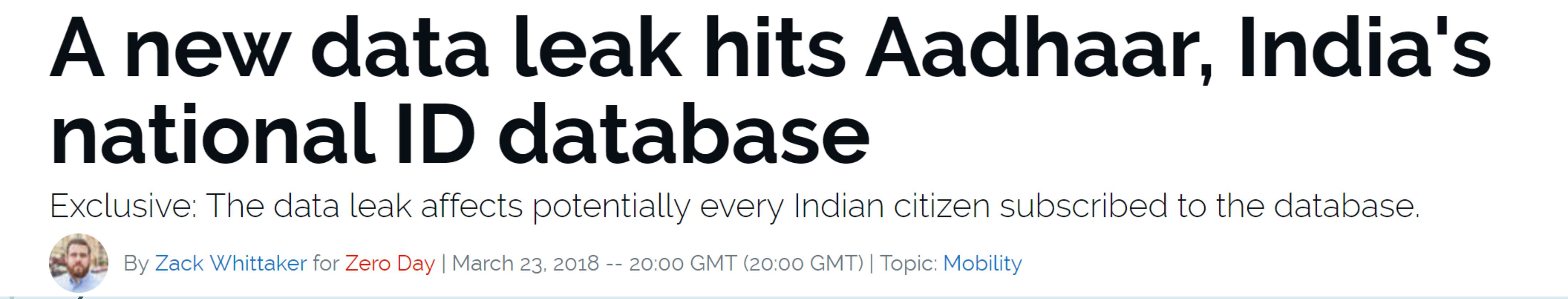
The next day, Alderson tweeted how the website of the Andhra Pradesh Panchayat Raj, a government body, had made publicly available the Aadhaar biometric data of thousands of citizens. Both the links directing to the Aadhaar data leaks were taken down after Alderson’s revelations.

More Leaks



The same day, Alderson exposed how the website of the English and Foreign Languages University publicly exhibited, without knowledge, the bank details, the voter identity card details, ration card details, and, of course, Aadhaar card details of not just the university's students but also the applicants during the pre-admission process.

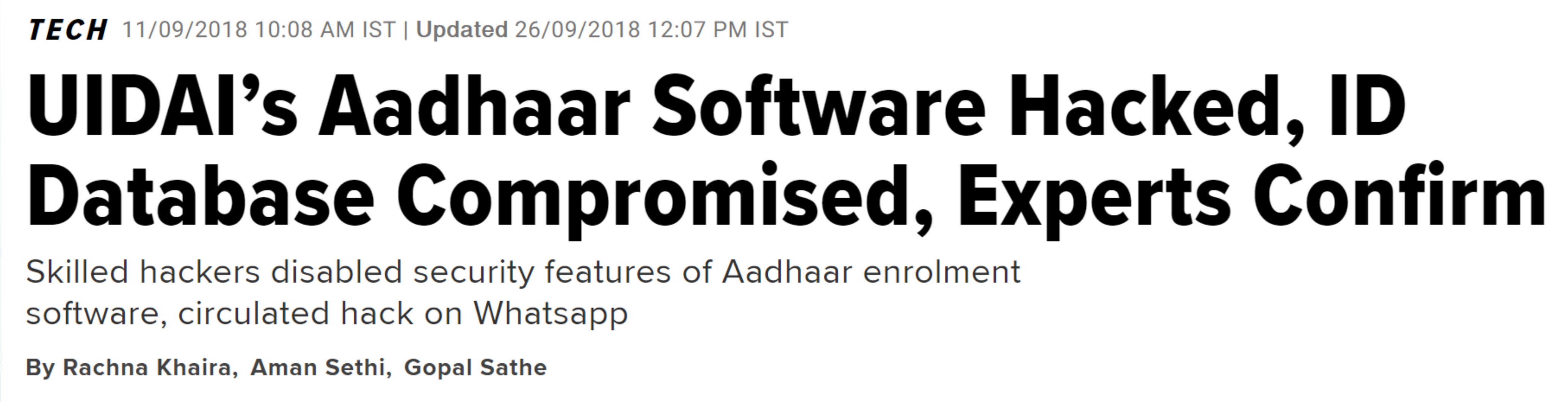
Some More Leaks



A new data leak hits Aadhaar, India's national ID database

Exclusive: The data leak affects potentially every Indian citizen subscribed to the database.

By Zack Whittaker for Zero Day | March 23, 2018 -- 20:00 GMT (20:00 GMT) | Topic: Mobility



TECH 11/09/2018 10:08 AM IST | **Updated** 26/09/2018 12:07 PM IST

UIDAI’s Aadhaar Software Hacked, ID Database Compromised, Experts Confirm

Skilled hackers disabled security features of Aadhaar enrolment software, circulated hack on Whatsapp

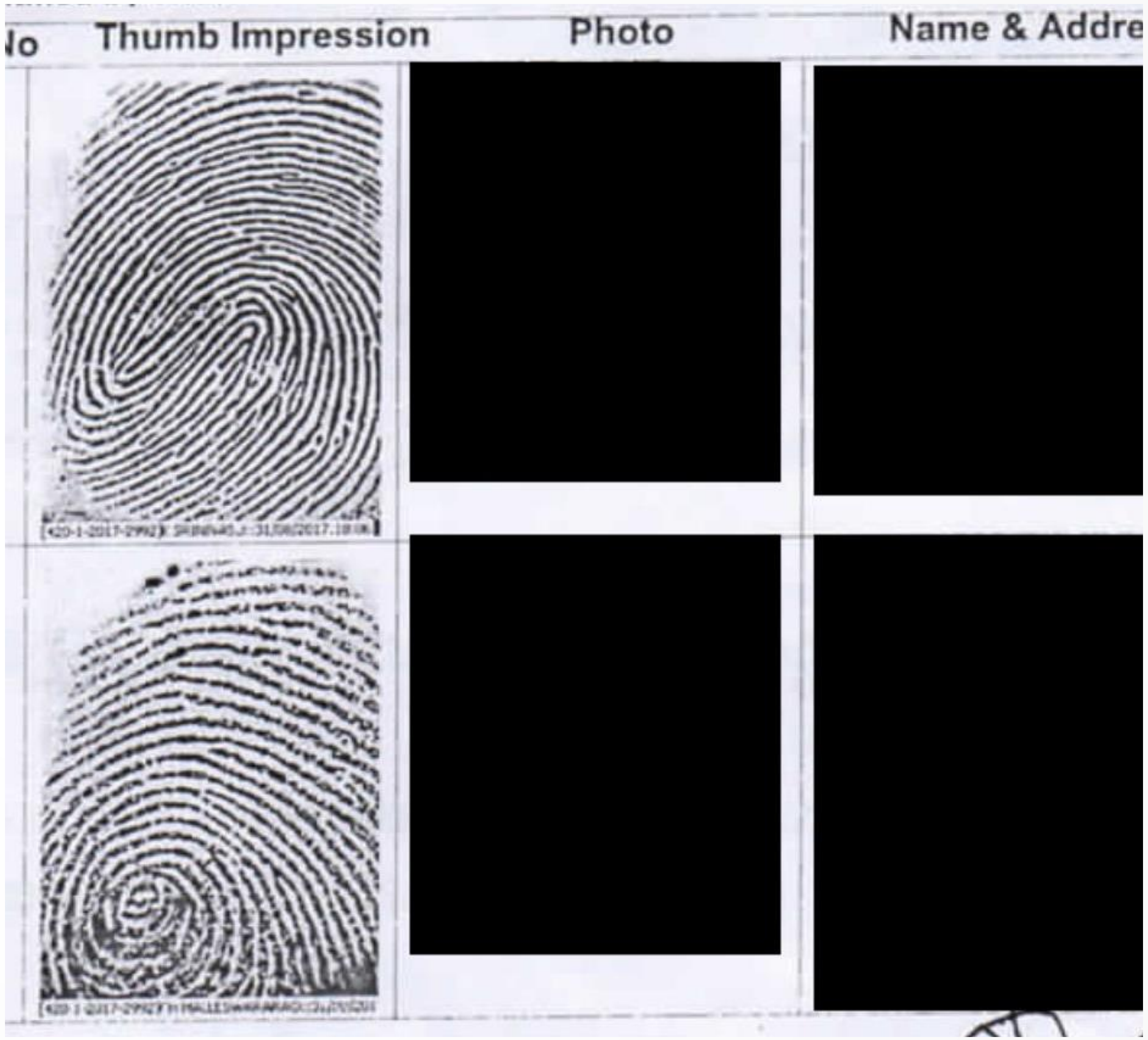
By Rachna Khaira, Aman Sethi, Gopal Sathe

That Last One

- Modified software patch that:
  - Disabled GPS checking
  - Lowered the sensitivity of the Iris recognition
- Create multiple fake cards easily.

- Could've been avoided if the system was server-side since its only meant to be accessed by those with authorisation.

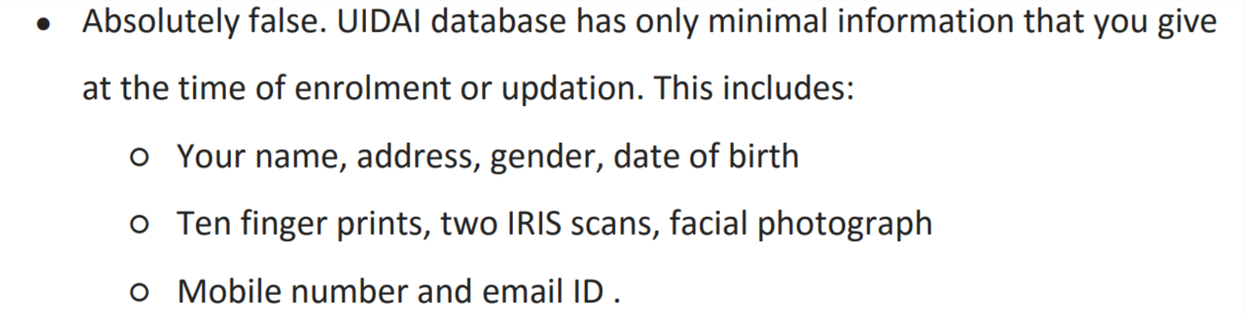
Storage of Sensitive Data



lo	Thumb Impression	Photo	Name & Addre
	[420-1-2017-29921 SRINIVAS.J :31/08/2017.18:08]	[redacted]	[redacted]
	[420-1-2017-29921 MALLESWARARAO.I:31/08/2017]	[redacted]	[redacted]

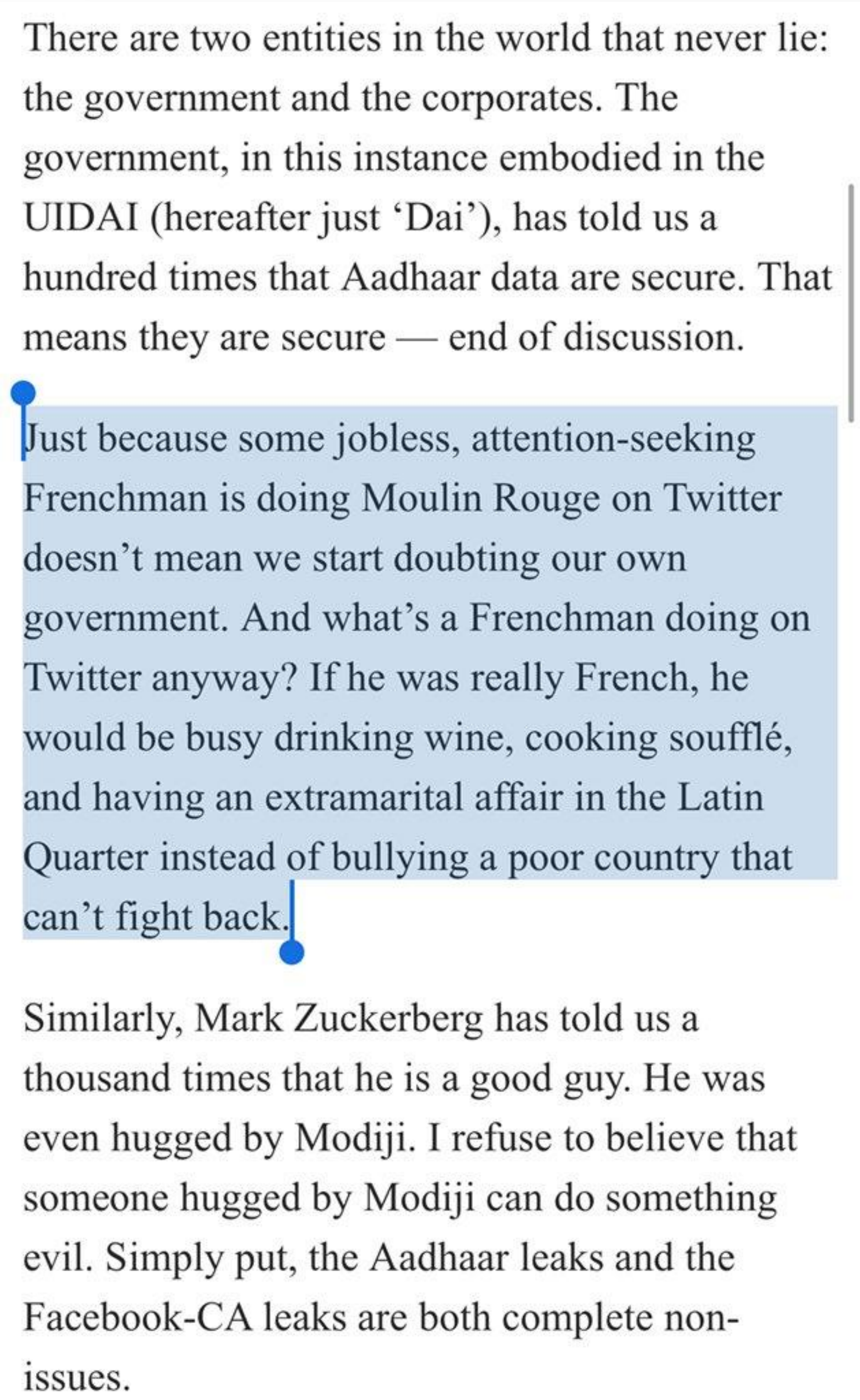
Conclusion

- Consumers are too willing to give unnecessary data
- No developer should believe their system is impenetrable
- Is the risk of storing all this data too great for the little convenience it creates?



- Absolutely false. UIDAI database has only minimal information that you give at the time of enrolment or updation. This includes:
  - Your name, address, gender, date of birth
  - Ten finger prints, two IRIS scans, facial photograph
  - Mobile number and email ID .

@fs0c131y vs. the world



There are two entities in the world that never lie: the government and the corporates. The government, in this instance embodied in the UIDAI (hereafter just ‘Dai’), has told us a hundred times that Aadhaar data are secure. That means they are secure — end of discussion.

Just because some jobless, attention-seeking Frenchman is doing Moulin Rouge on Twitter doesn’t mean we start doubting our own government. And what’s a Frenchman doing on Twitter anyway? If he was really French, he would be busy drinking wine, cooking soufflé, and having an extramarital affair in the Latin Quarter instead of bullying a poor country that can’t fight back.

Similarly, Mark Zuckerberg has told us a thousand times that he is a good guy. He was even hugged by Modiji. I refuse to believe that someone hugged by Modiji can do something evil. Simply put, the Aadhaar leaks and the Facebook-CA leaks are both complete non-issues.

Sources

- https://www.sbs.com.au/news/what-is-aadhaar-india-s-controversial-billion-strong-biometric-database
- https://factordaily.com/fsociety-interview-app-security-privacy/
- https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html
- https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/
- https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/
- https://scroll.in/magazine/872352/who-is-elliot-alderson-the-vigilante-hacker-taking-down-uidai-one-tweet-at-a-time