YISI LIU @ DIMENSION

Enhanced Privacy with Decentralized Identity

1. What is privacy?

BY DEFINITION

A FUNDAMENT RIGHT THAT IS ESSENTIAL TO AUTONOMY AND THE PROTECTION OF HUMAN DIGNITY

SPECIFICALLY

..THAT NO ONE WOULD EVER ASK YOU WHY YOU PUT A UNDERSTANDING THE LINUX KERNEL ON YOUR BOOK SHELF AT HOME

BECAUSE

THEY DO NOT AND SHOULD NEVER KNOW
THAT FACT

What happened in the past few years?

source: everywhere online

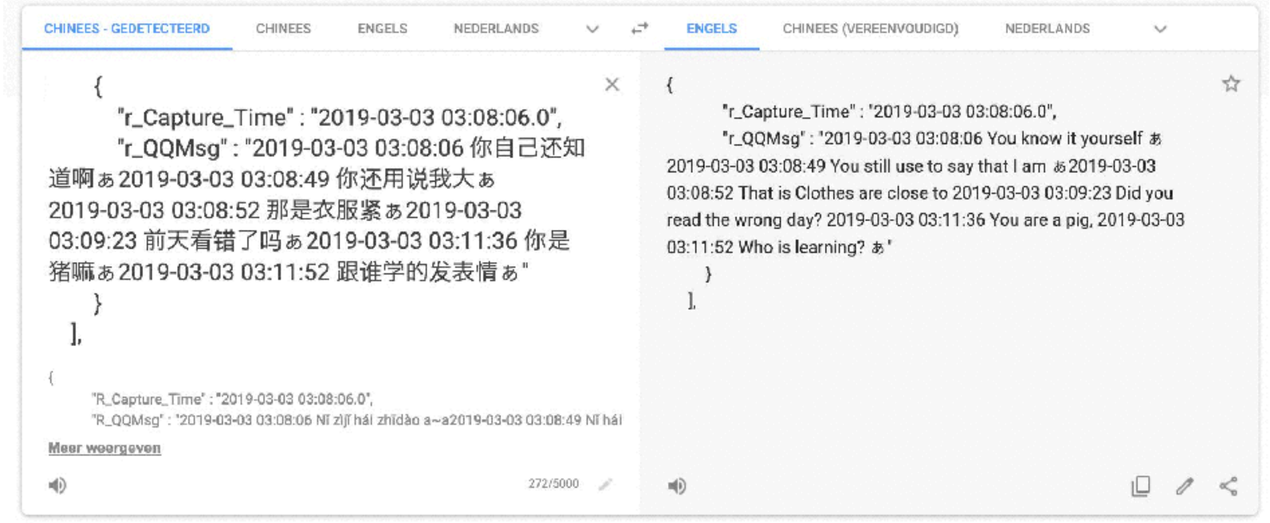
What happened in the past few years?

- Famous Facebook–Cambridge Analytica data scandal
- Up to ~87m users were affected
- Influenced 2016 American president election, 2016 Brexit and 2018 Mexican general election
- An "issue", a “mistake”, a "breach of trust” but not a “data breach”

source:https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html

What happened in the past few years?

- Equifax data breach
- ~145m users were affected in North America
- Highly sensitive personal data was leaked, including SSN, home address and credit card info
- A failure of secure implementation of their system



source: https://www.bleepingcomputer.com/news/security/open-mongodb-databases-expose-chinese-surveillance-data/

What happened in the past few years?

- WeChat Data Breach
- Over ~1 billion users are affected
- Over 300m Chinese private messages are exposed
- Governments are reported monitoring through both social media and instant messaging, not just in China
  - Tianyan Program
  - The Prism Project

Why is this important?

Rich Rogers
@RichRogersIoT

My wife asked me why I was speaking so softly at home.

I told her I was afraid Mark Zuckerberg was listening!

She laughed. I laughed.

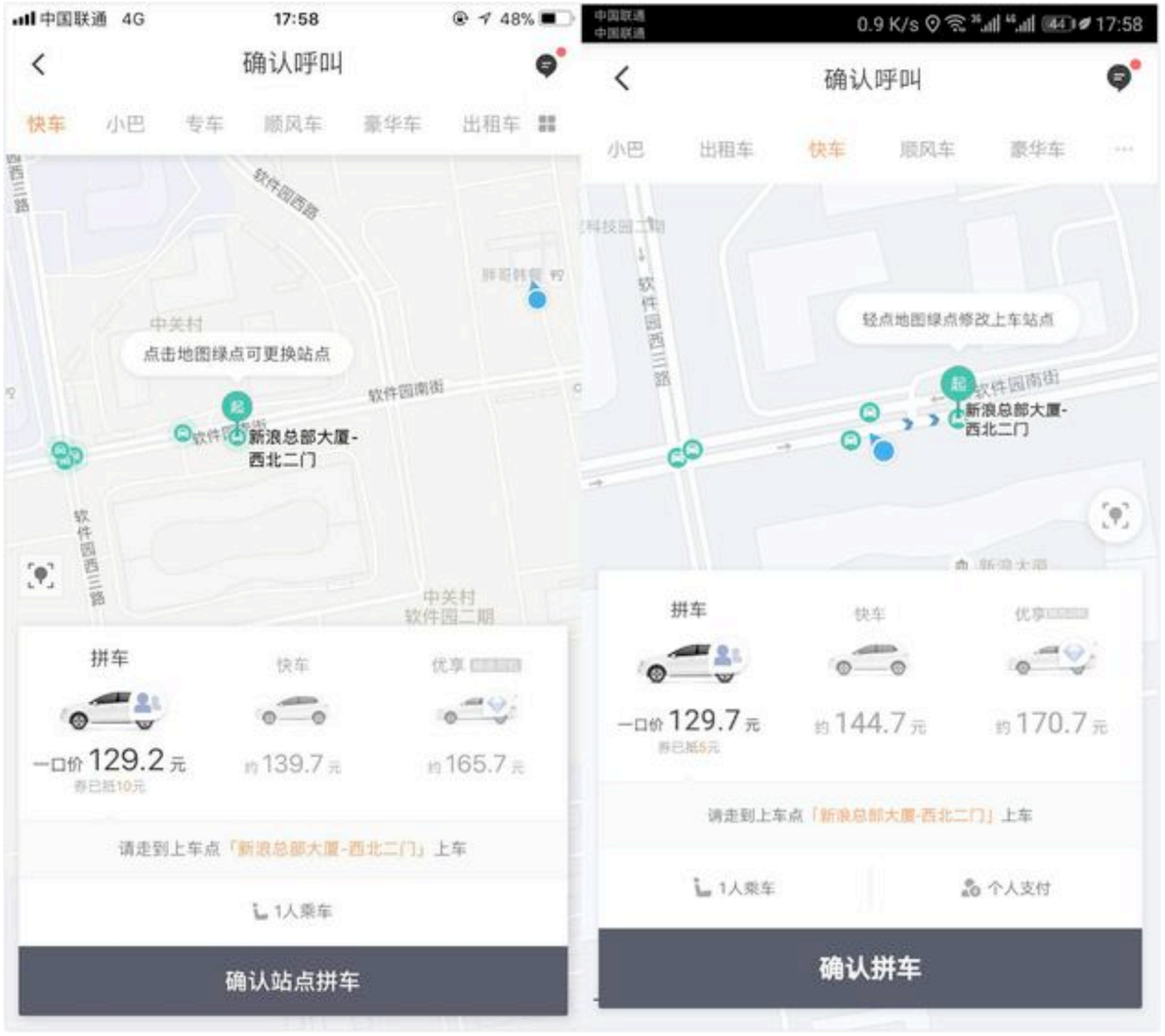
Alexa laughed. Siri laughed.

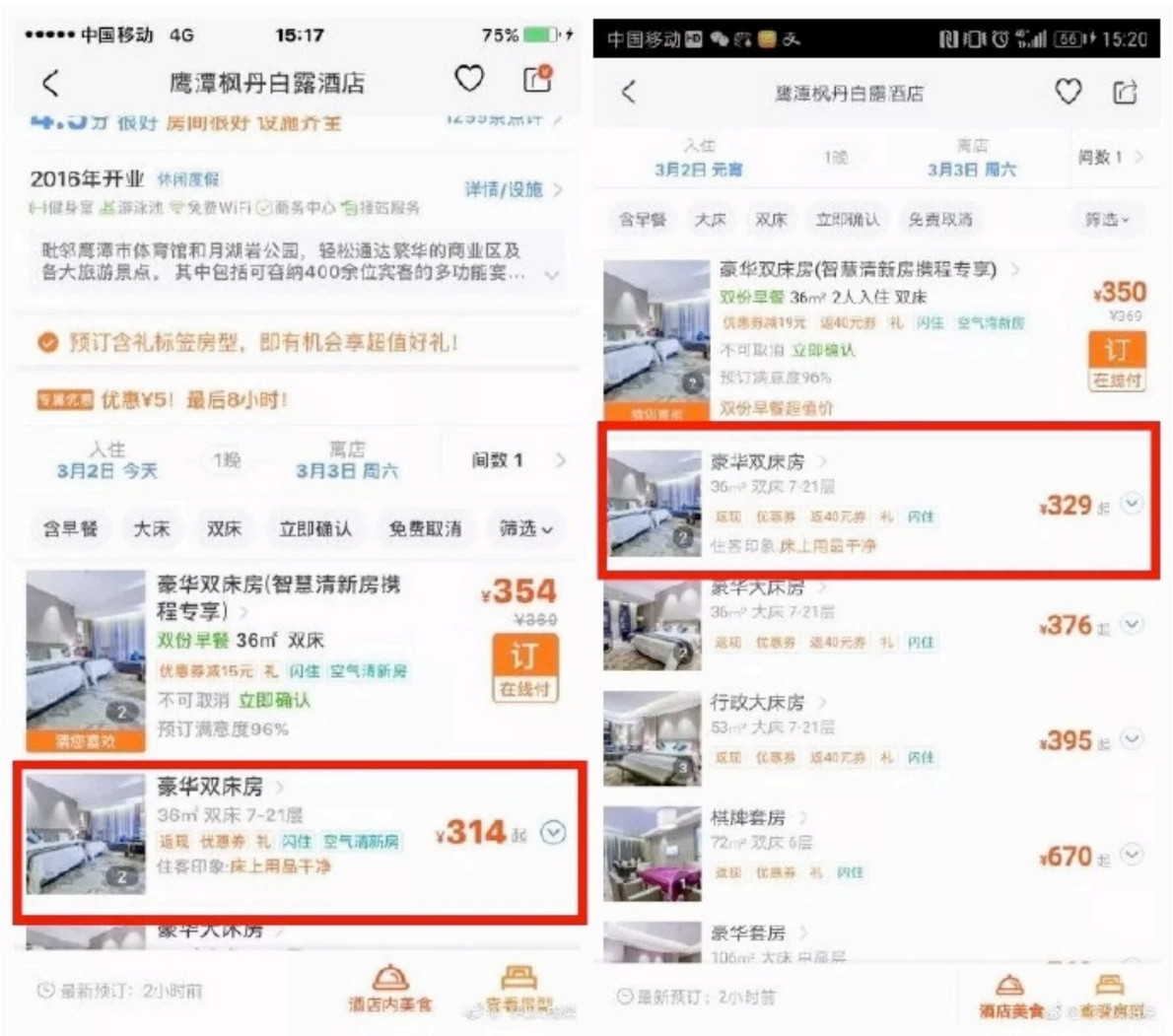
2:00 AM · Jun 2, 2019 · Twitter for iPhone

13.1K Retweets **48.6K** Likes

source: https://twitter.com/richrogersiot/status/1134973002196574209

source: https://medium.com/@pandaily/baidu-ceo-robin-li-chinese-consumers-favor-efficiency-at-the-expense-of-privacy-eea08bff9cb9





source: http://tech.sina.com.cn/i/2018-03-23/doc-ifysnevm2324295.shtml, http://www.szhgh.com/Article/news/society/2018-03-08/163275.html

Why is this important?

- We are under surveillance without being notified
- Our data is collected and shared across platform
- Our data, generated purely by ourselves, are used against us
- Our privacy is being violated without letting us aware of it

What has been done?

What has been done?

- General Data Protection Regulation(GDPR)
  - Privacy by design
  - No personal data is allowed to store on servers
  - Right to oblivion
- California Consumer Privacy Act (CCPA) in CA, USA
- Right to say no to personal data sales
- Right to know how personal data is used and how
- Right to equal service and price

GDPR So Far

Orgnization	Amount	Reasons
Google LLC	€ 50 million	Insufficient transparency, control, and consent over the processing of personal data for the purposes of behavioural advertising.
British Airways	£183 million	Use of poor security arrangements that resulted in a 2018 web skimming attack affecting 500,000 consumers.
Marriott International	£99 million	Failure to undertake sufficient due diligence when acquiring Starwood hotels group, whose systems where compromised in 2014, exposing approximately 339 million guest records.

2. What is identity?

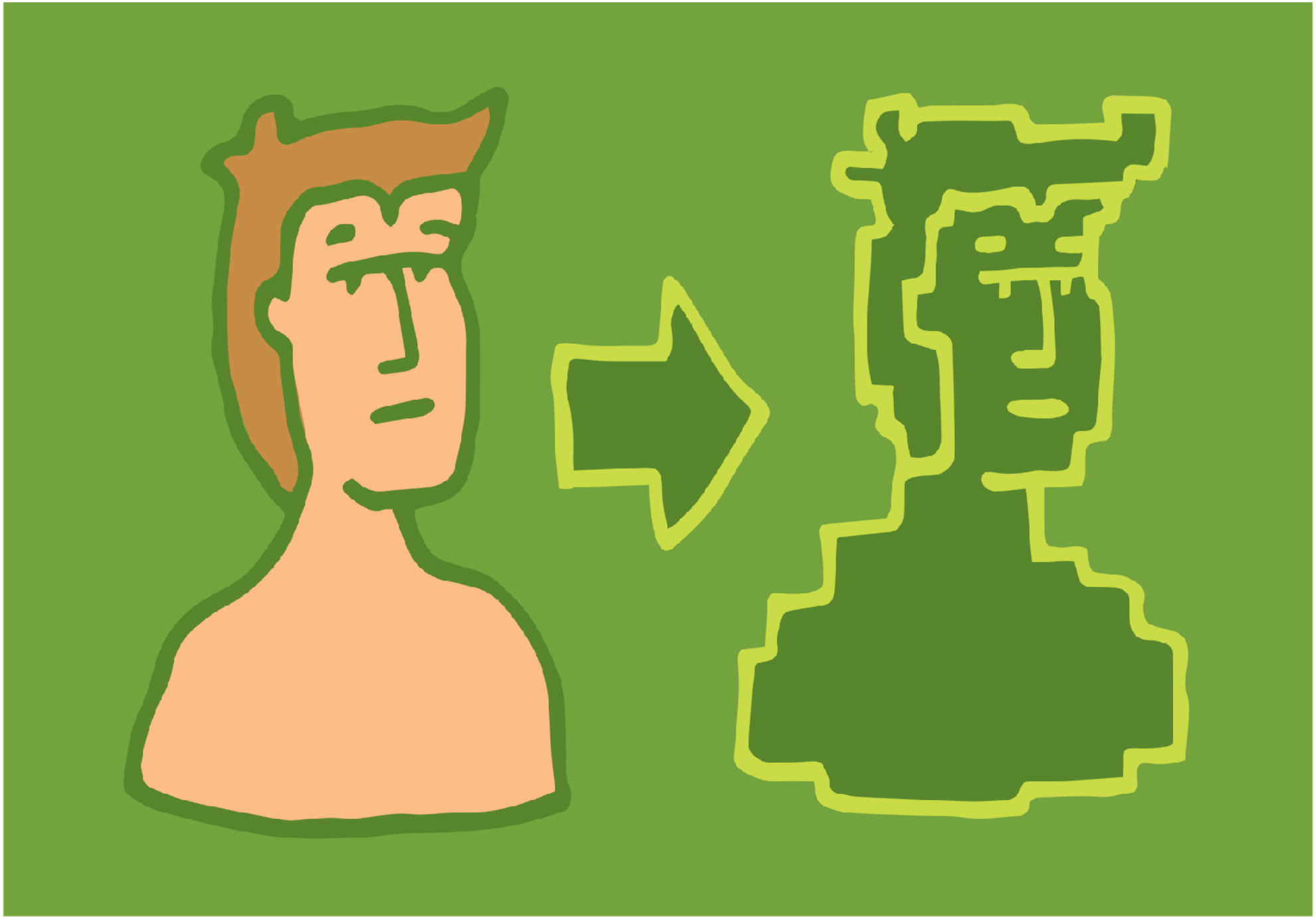
BY DEFINITION

IDENTITY IS THE QUALITIES, BELIEFS, PERSONALITY, LOOKS AND/OR EXPRESSIONS THAT MAKE A PERSON OR GROUP.

(photo cred: Individuality, The New Yorker June 2, 2014)

Social identity

- Social Identity is how you look like in the society
  - Your name
  - Your gender
  - Your nationality
  - Your occupation
- Verified by the government



Social identity

- The digital identity is how you look like on the Internet
  - Your Facebook account
  - Your Google account
  - Your Reddit account
- Verified by third-party organizations

What’s wrong with current digital identities?

What are the problems?

- The identity can be a key enabler to privacy
- The user identity's trust is largely dependent on the trust of the Identity providers
- Users need to register multiple accounts on different websites or services
- The identity providers are having too much access and control over users
- They are supposed to protect user's private information…

Different types of digital identities solutions

- One-to-one mapping
  - One account is corresponding to one platform
  - One needs to remember all his passwords to different platforms
  - Platforms control and store all the account information
    - Passwords
    - Personal information
    - Personal data

Facebook stored millions of Instagram passwords in plain text

A lot more than initially stated

By Jacob Kastrenakes | @jake_k | Apr 18, 2019, 3:02pm EDT

SHARE

Illustration by Alex Castro / The Verge

Notifying administrators about unhashed password storage

Suzanne Frey
VP, Engineering, Cloud Trust

May 21, 2019

Google's policy is to store your passwords with cryptographic hashes that mask those passwords to ensure their security. However, we recently notified a subset of our enterprise G Suite customers that some passwords were stored in our encrypted internal systems unhashed. This is a G Suite issue that affects business users only–no free consumer Google accounts were affected–and we are working with enterprise administrators to ensure that their users reset their passwords. We have been conducting a thorough investigation and have seen no evidence of improper access to or misuse of the affected G Suite credentials.

GitHub says bug exposed some plaintext passwords

A small but unspecified number of GitHub staff could have seen plaintext passwords.

By Zack Whittaker for Zero Day | May 1, 2018 -- 21:23 GMT (14:23 PDT) | Topic: Security

Twitter says bug exposed user plaintext passwords

Change your passwords — immediately.

By Zack Whittaker for Zero Day | May 3, 2018 -- 20:23 GMT (13:23 PDT) | Topic: Security

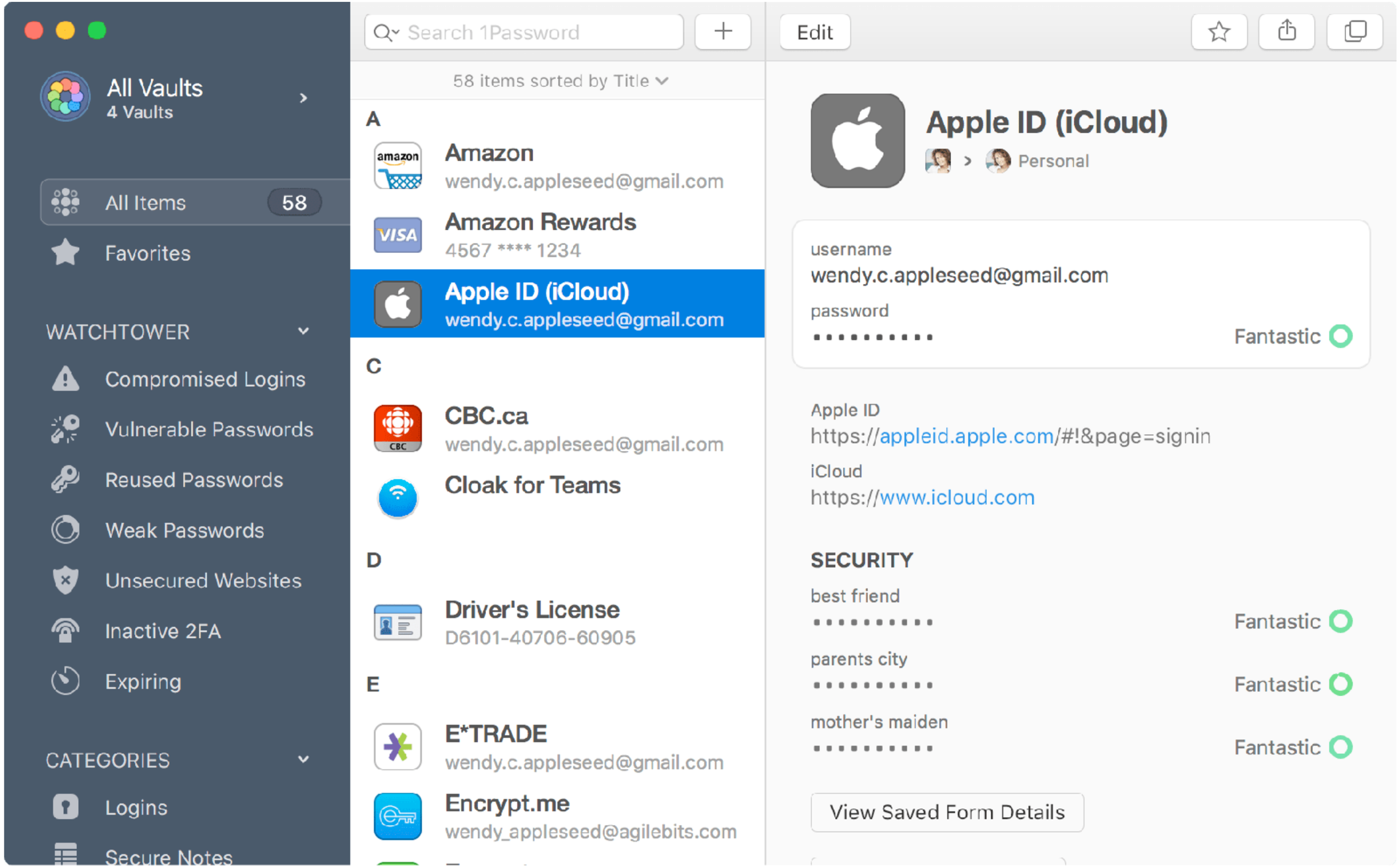
Robinhood Brokerage Firm Alerts of Passwords Stored in Clear Text

By Lawrence Abrams

July 24, 2019 05:57 PM 0

Different types of digital identities solutions

- One-to-one mapping
  - Password management tools - 1Password, LastPass
    - One needs to remember only **one** master password
    - Still need to register multiple accounts for multiple platforms
    - No unified identity

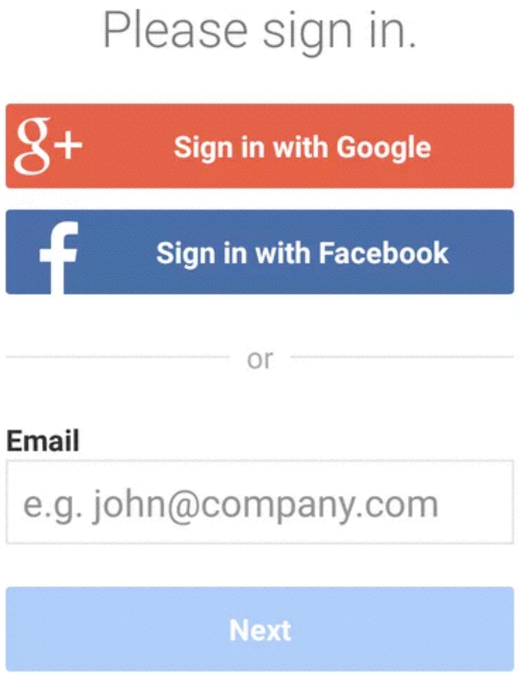

All Vaults
4 Vaults
All Items 58
Favorites
WATCHTOWER
Compromised Logins
Vulnerable Passwords
Reused Passwords
Weak Passwords
Unsecured Websites
Inactive 2FA
Expiring
CATEGORIES
Logins
Secure Notes
Search 1Password
58 items sorted by Title
A
Amazon
wendy.c.appleseed@gmail.com
Amazon Rewards
4567 **** 1234
Apple ID (iCloud)
wendy.c.appleseed@gmail.com
C
CBC.ca
wendy.c.appleseed@gmail.com
Cloak for Teams
D
Driver's License
D6101-40706-60905
E
E*TRADE
wendy.c.appleseed@gmail.com
Encrypt.me
wendy_appleseed@agilebits.com
Edit
Apple ID (iCloud)
Personal
username
wendy.c.appleseed@gmail.com
password
Fantastic
Apple ID
https://appleid.apple.com/#!&page=signin
iCloud
https://www.icloud.com
SECURITY
best friend
Fantastic
parents city
Fantastic
mother's maiden
Fantastic
View Saved Form Details

Different types of digital identities solutions

- One-to-many mapping
  - One account can authorize multiple platforms
  - One only needs to remember **one** password for his master account
  - Personal information is only stored on the master account
  - Personal data is still stored on multiple platforms

Different types of digital identities solutions

- One-to-many mapping
  - OpenID - Google Login, Facebook Login, Twitter Login
    - Single Sign On(SSO)
    - Unified identity
    - Trust is dependent on the Identity Provider(IdP)



What’s lost here?

IDENTITIES ARE STILL CENTRALIZED
AND CONTROLLED BY THIRD-PARTIES

Different types of digital identities solutions

- Many-to-many mapping
  - One account can authorize multiple platforms - one-to-many
  - Unlimited number of accounts for one platform - many-to-one
  - Combined together - many-to-many
  - One can create identities at any time without any restriction
  - Personal information is controlled by the account owner
  - Personal data is still stored on different platforms

Different types of digital identities solutions

- Many-to-many mapping
  - Decentraized Identity
    - A cryptographic key pair
    - Creation only requires math
    - No need to be verified by third parties
    - Control which information to share with which platform

Decentralized Identifiers(DIDs)

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // this key can be used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "service": [{
    "id": "did:example:123456789abcdefghi#service123",
    "type": "ExampleService",
    "serviceEndpoint": "https://example.com/endpoint/8377464"
  }]
}
```

Where’s the trust?

Where's the trust?

- Blockchain, or more generally, distributed ledger technology (DLT)
- Each identity is stored on DLTs
- Each validation on different services or platforms is also updated on DLTs
- The trust is built upon these globally distributed ledgers or decentralized P2P networks
- The trust of Mathematics

Where’s the privacy then?

Where's the privacy?

- DIDs eliminate the control from third parties over users
- However, the data is still being collected by them
- DIDs cannot solve the data surveillance and abuse problems
  - Solid(https://solid.mit.edu) offers a interesting and radical solution
  - One's data is stored in their personal "pod"(personal online data stores)
  - Applications no longer store and "own" user data

3. Can we really opt-out?

WE CAN, BUT NOT EVERYONE

Our Attempts

- To enable users to control their privacy over the online platforms
- We don’t build our own platforms - we build upon existing ones
- Privacy-ensured social network solution - Maskbook
- Privacy-ensured instant messaging solution - Tessercube

Maskbook

- What is Maskbook?
  - A browser extension
  - Each user with an unified identity (secp256k1 key pair) and link it to their Facebook account
  - Create encrypted posts that only designated friends can decrypt
  - Hide from no one but Facebook

Maskbook

- Why Maskbook?
  - We might have nothing to hide.
  - But we also have nothing to surrender.
  - And they must have nothing to steal.

Yisi Liu

Update Info 1 | Activity Log 2 | ...

Timeline | About | Friends 499 | Photos | Archive | More

2 items for you to review

Intro

A8cEYX3FvuU8HmpDrtrxKFHdTLn505gT2t7JdMjHDu5K

- Studied at University of Illinois at Urbana-Champaign
- Went to Fuxing Senior High School
- Went to 上海市复兴中学 Shanghai Fuxing High School 上海市复兴高级中学
- Went to Fuxing High School
- Went to 上海市复兴高级中学
- Lives in Urbana, Illinois
- From Shanghai, China
- Followed by 7 people

Create Post | Photo/Video | Live Video | Life Event

What's on your mind?

Photo/Video | Tag Friends | Feeling/Activ... | ...

Posts | Manage Posts | List View | Grid View

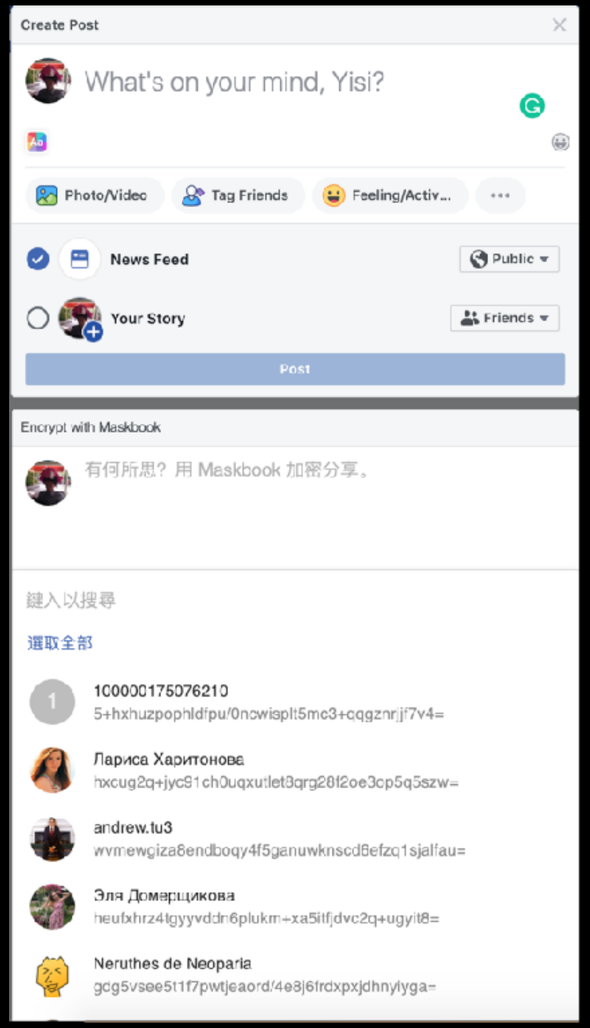
Yisi Liu
5 mins ·

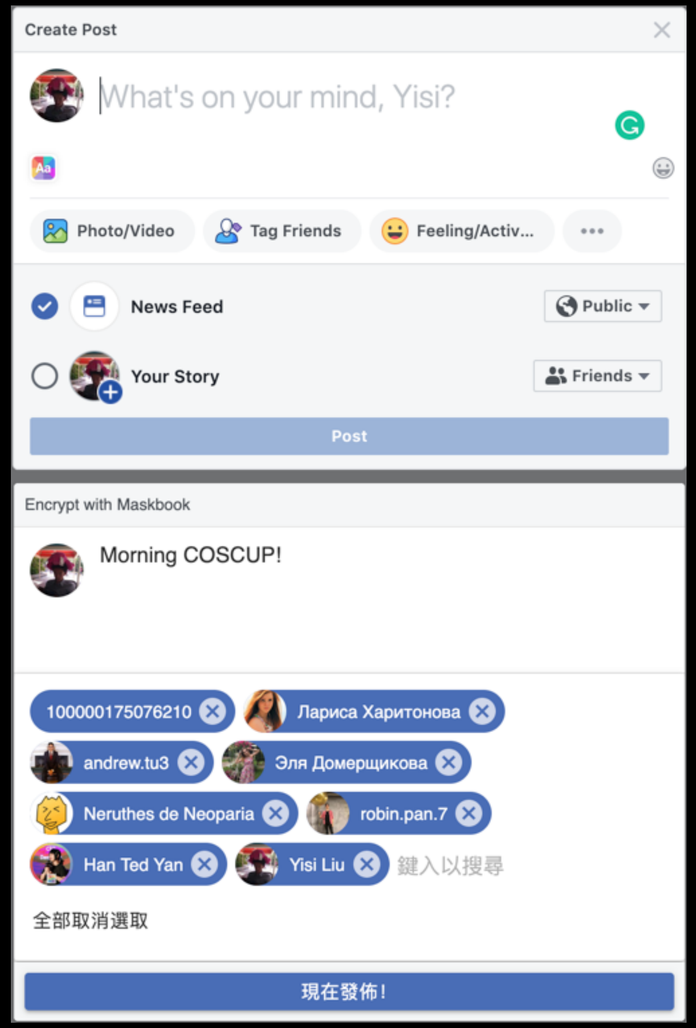
來 Maskbook 解密這個訊息！

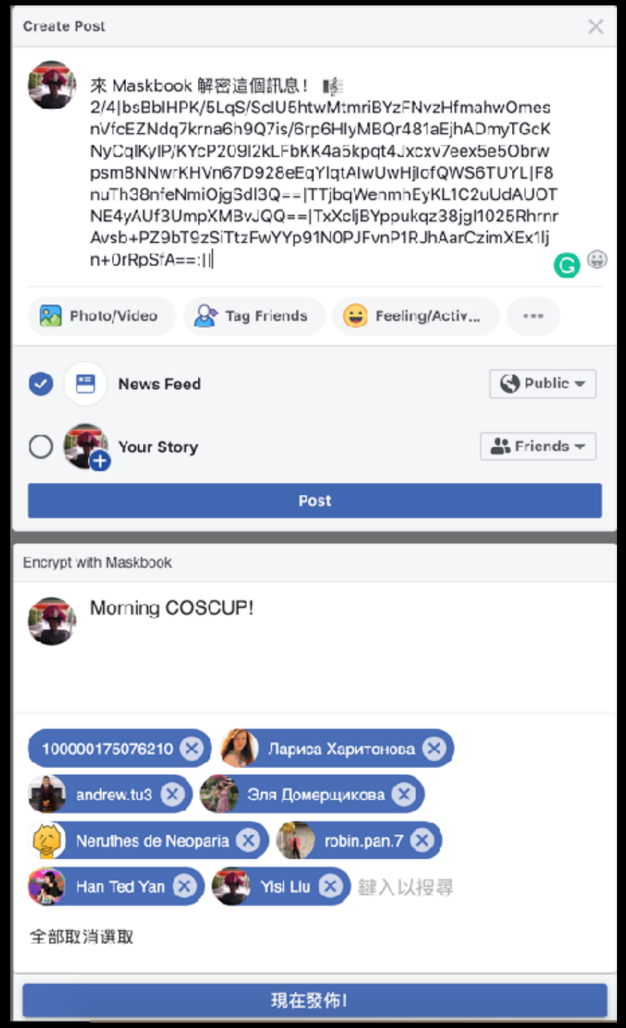
Maskbook 解密出的文本: 查看或添加收件人 數字簽名驗證成功 ✔

Morning COSCUP!

Like | Comment | Share

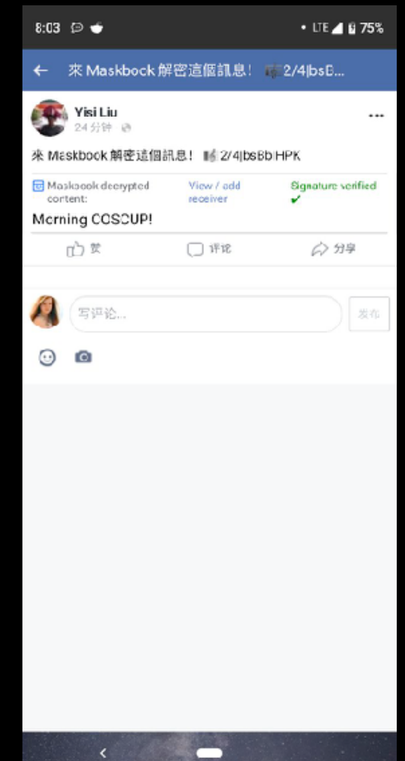

Create Post
What's on your mind, Yisi?
Photo/Video
Tag Friends
Feeling/Activ...
News Feed
Public
Your Story
Friends
Post
Encrypt with Maskbook
有何所思？用 Maskbook 加密分享。
鍵入以搜尋
選取全部
100000175076210
5+hxhuzpophldfpu/0ncwispit5mc3+cqgznrjjf7v4=
Лариса Харитонова
hxcug2q+jyc91ch0uqxutlet3qrg28f2oe3cp5q5szw=
andrew.tu3
wvmewgiza6endboqy4f5ganuwknscd6efzq1sjalfau=
Эля Домерщикова
heufxhrz4tgyyvddn6plukm+xa5itfjdvc2q+ugyit8=
Neruthes de Neoparia
gcg5vsee5t1f7pwtjeaord/4e8j6frdxpxjdhnylyga=

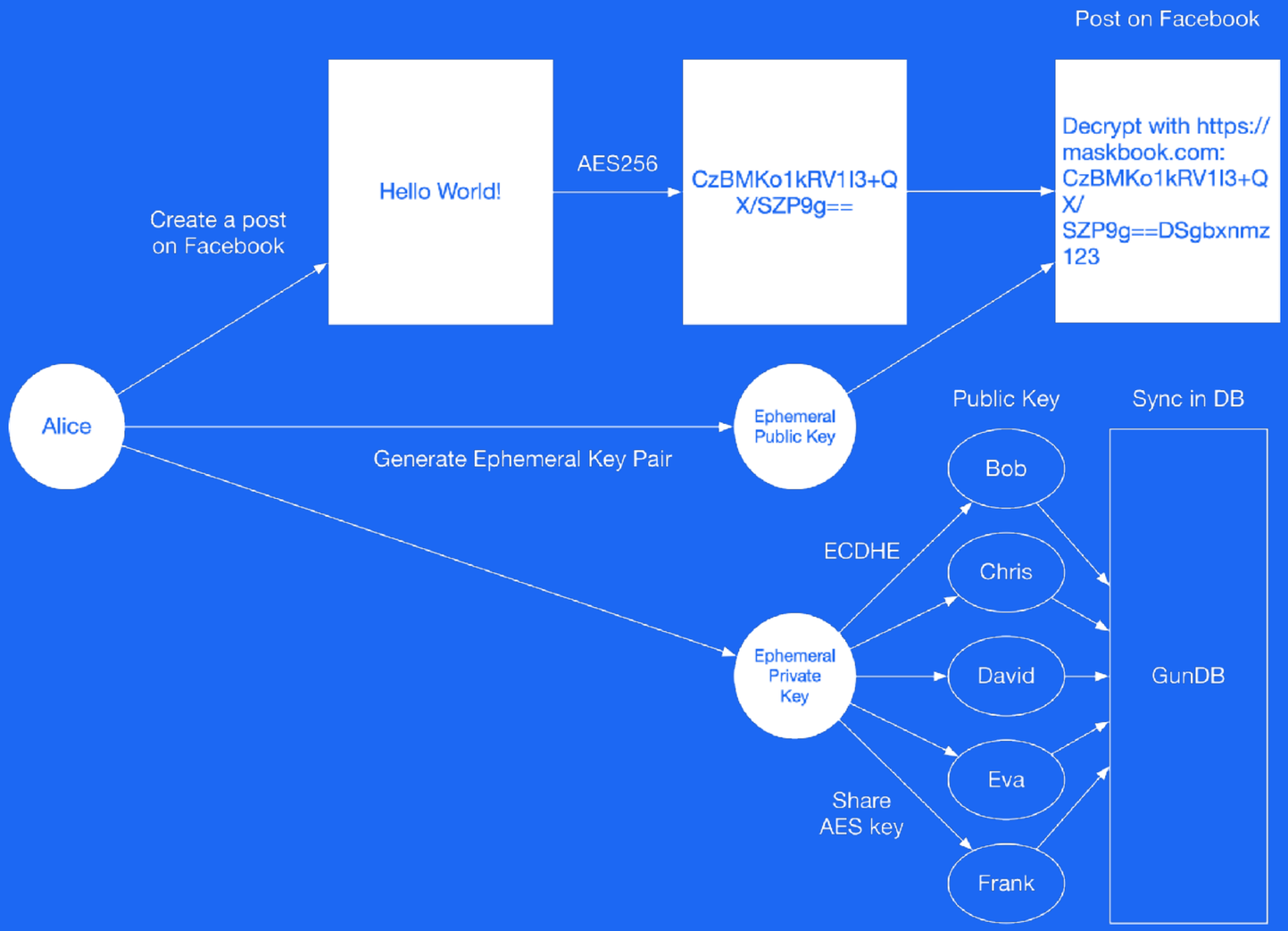

Create Post
What's on your mind, Yisi?
Photo/Video
Tag Friends
Feeling/Activ...
News Feed
Public
Your Story
Friends
Post
Encrypt with Maskbook
Morning COSCUP!
100000175076210
Лариса Харитонова
andrew.tu3
Эля Домерщикова
Neruthes de Neoparia
robin.pan.7
Han Ted Yan
Yisi Liu
鍵入以搜尋
全部取消選取
現在發佈!


Create Post
來 Maskbook 解密這個訊息！
2/4|bsBbIHPK/5LqS/SclU5htwMtmriBYzFNvzHfmahwOmesnVfcEZNdq7krna6h9Q7is/6rp6HIyMBQr481aEjhADmyTGcKNyCqIKyIPjKYcP209l2kLFbKK4a5kpqt4Jxcxv7eex5e5Obrwpsm8NNwrKHVn67D928eEqYlqtAlwUwHjlofQWS6TUYL|F8nuTh38nfeNmiOjgSdl3Q==|TTjbqWenmhEyKL1C2uUdAUOTNE4yAUf3UmpXMBvJQQ==|TxXcljBYppukqz38jgl1025RhrnrAvsb+PZ9bT9zSiTtzFwYYp91N0PJFvnP1RJhAarCzimXEx1ljn+0rRpSfA==:||
Photo/Video
Tag Friends
Feeling/Activ...
News Feed
Public
Your Story
Friends
Post
Encrypt with Maskbook
Morning COSCUP!
100000175076210
Лариса Харитонова
andrew.tu3
Эля Домерщикова
Neruthes de Neoparia
robin.pan.7
Han Ted Yan
Yisi Liu
鍵入以搜尋
全部取消選取
現在發佈!


Uploading...
Yisi Liu
Just now
來 Maskbook 解密這個訊息！
2/4|bsBbIHPK/5LqS/SclU5htwMtmriBYzFNvzHfmahwOmesnVfcEZNdq7krna6h9Q7is/6rp6HIyMBQr481aEjhADmyTGcKNyCqIKyIPjKYcP209l2kLFbKK4a5kpqt4Jxcxv7eex5e5Obrwpsm8NNwrKHVn67D928eEqYlqtAlwUwHjlofQWS6TUYL|F8nuTh38nfeNmiOjgSdl3Q==|TTjbqWenmhEyKL1C2uUdAUOTNE4yAUf3UmpXMBvJQQ==|TxXcljBYppukqz38jgl1025RhrnrAvsb+PZ9bT9zSiTtzFwYYp91N0PJFvnP1RJhAarCzimXEx1jn+0rRpSfA==:||


Yisi Liu
Just now
來 Maskbook 解密這個訊息！
Maskbook 解密出的文本:
查看或添加收件人
數字簽名驗證成功
Morning COSCUP!
Like
Comment
Share


8:03
LTE 75%
來 Maskbook 解密這個訊息！ 2/4|bsB...
Yisi Liu
24 分钟
來 Maskbook 解密這個訊息！ 2/4|bsBbIHPK
Maskbook decrypted content:
View / add receiver
Signature verified
Morning COSCUP!
赞
评论
分享
写评论...
发布

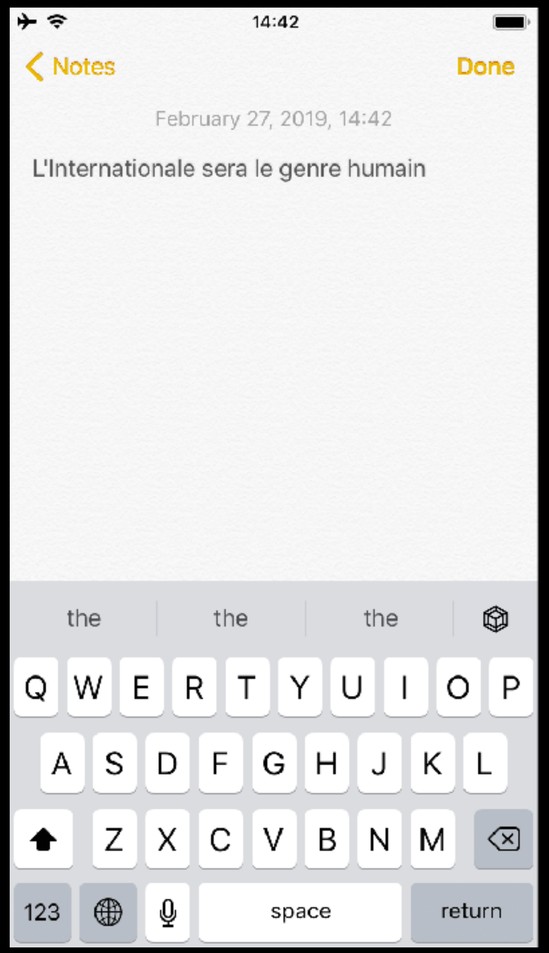

Post on Facebook
Hello World!
AES256
CzBMKo1kRV1l3+Q
X/SZP9g==
Decrypt with https://
maskbook.com:
CzBMKo1kRV1l3+Q
X/
SZP9g==DSgbxnmz
123
Create a post
on Facebook
Alice
Ephemeral
Public Key
Generate Ephemeral Key Pair
Public Key
Sync in DB
Bob
Chris
David
Eva
Frank
ECDHE
Ephemeral
Private
Key
Share
AES key
GunDB

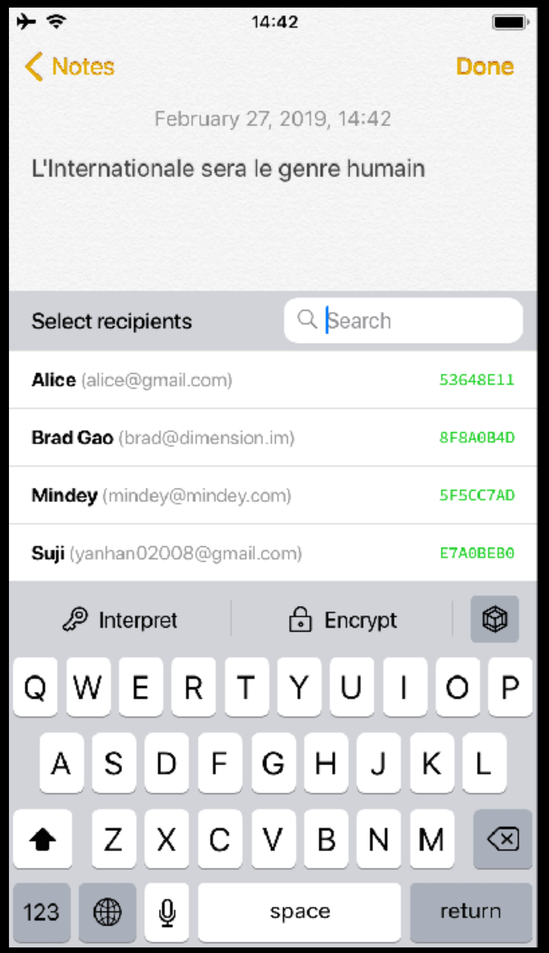
Tessercube

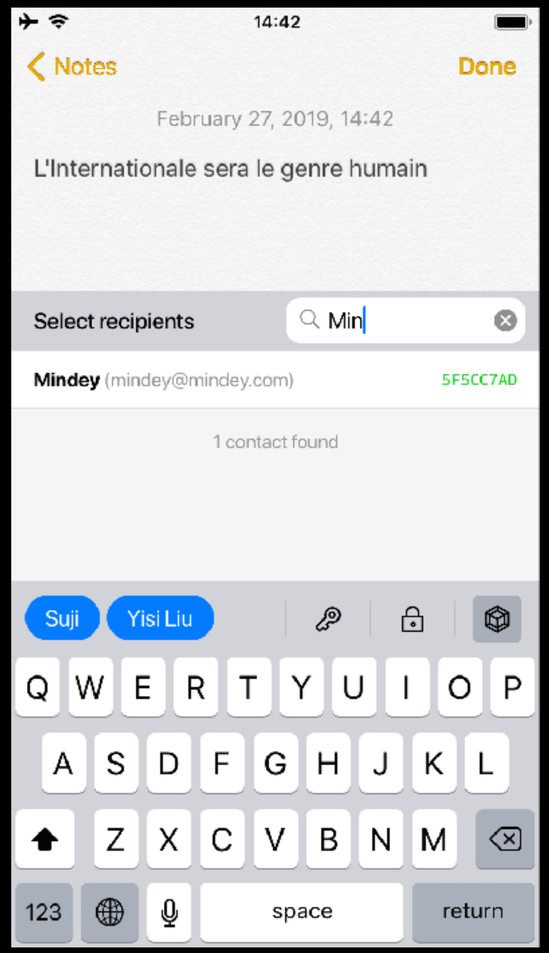
- What is Tessercube?
  - A mobile keyboard (input method)
  - Enabling users to encrypt any text and decrypt cipher text in all text input fields

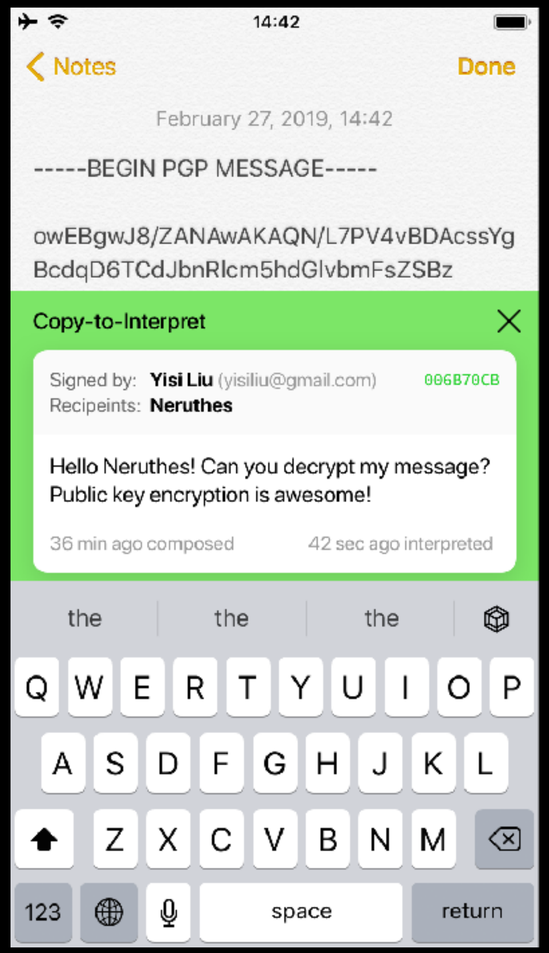
Tessercube

- Why Tessercube?
  - End2End Encryption (E2EE) communications
  - You can protect all your sensitive messages from being accessed by platforms
  - You can realize E2EE anywhere, not just in Signal or WhatsApp


14:42
Notes
Done
February 27, 2019, 14:42
L'Internationale sera le genre humain
the
the
the
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return


14:42
Notes
Done
February 27, 2019, 14:42
L'Internationale sera le genre humain
Select recipients
Search
Alice (alice@gmail.com) 53648E11
Brad Gao (brad@dimension.im) 8F8A0B4D
Mindey (mindey@mindey.com) 5F5CC7AD
Suji (yanhan02008@gmail.com) E7A0BEB0
Interpret
Encrypt
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return


14:42
Notes
Done
February 27, 2019, 14:42
L'Internationale sera le genre humain
Select recipients
Min
Mindey (mindey@mindey.com) 5F5CC7AD
1 contact found
Suji
Yisi Liu
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return


14:42
Notes
Done
February 27, 2019, 14:42
-----BEGIN PGP MESSAGE-----
owEBgwJ8/ZANAwAKAQN/L7PV4vBDAcssYg
BcdqD6TCdJbnRlcm5hdGlvbmFsZSBz
Copy-to-Interpret
Signed by: Yisi Liu (yisiliu@gmail.com) 006B70CB
Recipeints: Neruthes
Hello Neruthes! Can you decrypt my message?
Public key encryption is awesome!
36 min ago composed
42 sec ago interpreted
the
the
the
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return

Comparison	Allo	iMessage	Messenger	Riot	Signal	Skype	Telegram	Threema	Viber	Whatsapp	Wickr	Wire
TL;DR: Does the app secure my messages and attachments?	No	No	No	No	Yes	No	No	Yes	No	No	No	Yes
Company jurisdiction	USA	USA	USA	UK	USA	USA	USA / UK / Belize	Switzerland	Luxembourg / Japan	USA	USA	Switzerland
Infrastructure jurisdiction	USA, Belgium, Finland, Ireland,the Netherlands, Chile, Taiwan,and Singapore	USA (Ireland and Denmark planned); iMessage runs on AWS and Google Cloud	USA, Sweden (Ireland planned)	UK (and potentially all jurisdictions, given it's a decentralised messaging platform)	USA	USA, the Netherlands, Australia, Brazil, China, Ireland, Hong Kong, and Japan	UK, Singapore, USA, and Finland	Switzerland	USA	USA (unsure of other locations)	USA (unsure of other locations)	Germany / Ireland
Implicated in giving customers' data to intelligence agencies?	Yes	Yes	Yes	No	No	Yes	No	No	No	Yes	No	No
Surveillance capability built into the app?	No	No	No	No	No	Yes	No	No	No	No	No	No
Does the company provide a transparency report?	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Company's general stance on customers' privacy	Poor	Poor	Poor	Good	Good	Poor	Poor	Good	Poor	Poor	Good	Good
Funding	Google	Apple	Facebook	New Vector Limited	Freedom of the Press Foundation, the Knight Foundation, the Shuttleworth Foundation, and the Open Technology Fund, Signal Foundation (Brian Acton)	Microsoft	Pavel Durov	User pays	Rakuten, friends and family of Talmon Marco (it's very unclear)	Facebook	Gilman Louie, Juniper Networks, the Knight Foundation, Breyer Capital, CME Group, and Wargaming	Janus Friis, Iconical, Zeta Holdings Luxembourg
Company collects customers' data?	Yes	Yes	Yes	No	No	Yes	Yes	No	Yes	Yes	No	No
App collects customers' data?	Yes	Yes	Yes	Minimal	Minimal	Yes	Yes	No	Yes	Yes	No	Minimal

source: https://www.securemessagingapps.com

Tessercube

- How does Tessercube work?
  - For now, we are complying with OpenPGP Standard (RFC 4880)
  - In our next version, we are forcing users to use Elliptic Curve Cryptography(ECC) for better user experience

Decentralized Identity

- One can bring their own ECC key to both Maskbook and Tessercube
- One's social account is apart from their keys, their **real** identities
- Different key pairs as different **personas**
- Personas have their own permission system for forming a new network

Why did we choose this path?

Can we really opt-out?

- People are not willing to quit or leave their comfort zone, such as Facebook, Twitter, or Messenger, WhatsApp, Telegrem
- We provide users a **opt-out** option to protect their privacies, without forcing them to leave their comfort zone
- We provide users an easy access into crypto-anarchy
- We convert existing Internet giant platforms into infrastructures, like what we did with HTTP and HTTPS

source: https://gimmemojo.com/2017/08/23/buyer-personas-telecom-channel/

FIND US ON

MASKBOOK.COM

TESSERCUBE.COM

GITHUB.COM/DIMENSIONDEV