

YISI LIU @ DIMENSION

---

**Enhanced Privacy with  
Decentralized Identity**

# 1. What is privacy?

BY DEFINITION

A FUNDAMENTAL 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 a  
few years?**



source: everywhere online

## What happened in the past a 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 a 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



Victor Gevers  
@0xDUDE

The most dialogs which are being monitored are typical teenager conversations. Which conversations need to be reviewed by a human based on "trigger words" is at this moment still not entirely clear.

CHINEES - GEDETEECTEERD CHINEES ENGELS NEDERLANDS ENGELS CHINEES (VEREENVOUDIGD) NEDERLANDS

```
[{"r_Capture_Time": "2019-03-03 03:08:06.0", "r_QQMsg": "2019-03-03 03:08:06 你自己还知道啊 2019-03-03 03:08:49 你还用说大啊 2019-03-03 03:08:52 那是衣服紧 2019-03-03 03:09:23 前天看错了吗 2019-03-03 03:11:36 你是猪嘛 2019-03-03 03:11:52 跟谁学的表情啊"}, {"r_Capture_Time": "2019-03-03 03:08:06.0", "r_QQMsg": "2019-03-03 03:08:06 You know it yourself ah 2019-03-03 03:08:49 You still use to say that I am ah 2019-03-03 03:08:52 That is Clothes are close to 2019-03-03 03:09:23 Did you read the wrong day? 2019-03-03 03:11:36 You are a pig, 2019-03-03 03:11:52 Who is learning? ah"}]
```

8:27 PM · Mar 2, 2019 from Beijing, People's Republic of China · Twitter Web Client

209 Retweets 368 Likes

CHINEES - GEDETEECTEERD CHINEES ENGELS NEDERLANDS ENGELS CHINEES (VEREENVOUDIGD) NEDERLANDS

```
[{"r_Capture_Time": "2019-03-03 03:08:06.0", "r_QQMsg": "2019-03-03 03:08:06 你自己还知道啊 2019-03-03 03:08:49 你还用说大啊 2019-03-03 03:08:52 那是衣服紧 2019-03-03 03:09:23 前天看错了吗 2019-03-03 03:11:36 你是猪嘛 2019-03-03 03:11:52 跟谁学的表情啊"}, {"r_Capture_Time": "2019-03-03 03:08:06.0", "r_QQMsg": "2019-03-03 03:08:06 You know it yourself ah 2019-03-03 03:08:49 You still use to say that I am ah 2019-03-03 03:08:52 That is Clothes are close to 2019-03-03 03:09:23 Did you read the wrong day? 2019-03-03 03:11:36 You are a pig, 2019-03-03 03:11:52 Who is learning? ah"}]
```

8:27 PM · Mar 2, 2019 from Beijing, People's Republic of China · Twitter Web Client

209 Retweets 368 Likes

```
{"_index": "url_0", "type": "url", "id": "f671ba4d-4726-40a9-ad7f-ecb21851c653", "score": 1, "source": {"unitstype": "0", "Auth_Type": "1021111", "Auth_Account": "", "Session_ID": "6E21A90DBCBD48B286D6AF730EB26E80", "IDName": "", "Certificate": "111", "CertificateNo": "", "Capture_Time": "2019-03-02T18:56:08.000Z", "InstDateTime": "2019-03-02T18:56:27.000Z", "SeatIp": "", "SeatNo": "", "ID": "CB8959R001", "LabelNub": "", "Terminal_Mac": "", "Terminal_Mac_terms": "", "URL": "http://cf.qq.com/act/a20180408ingame/other.htm", "url_terms": "cf.qq.com", "Title": "http://cf.qq.com/act/a20180408ingame/other.htm", "Longitude": "120.146646", "Latitude": "33.371189", "Device_Num": "th0200", "Device_Mac": "", "Device_Mac_terms": "", "Site_Code": "th0200", "site_code_terms": "th0200", "Site_Name": "新苹果网吧", "Area": "0001", "PoliceStation": "1001", "OrgCode": "55080760X", "TypeID": 1, "address": "盐南西路4号", "device_class": "", "PersonType": [], "PersonNo": "0", "Source": "120", "systemtime": "2019-03-02T19:15:41.000Z"}}, {"_index": "url_1", "type": "url", "id": "d54931a1-874c-49dc-924b-2d44cbcd0b68", "score": 1, "source": {"unitstype": "0", "Auth_Type": "1021111", "Auth_Account": "", "Session_ID": "6981BEAC52324BB6A38CCBAC0CA0D804", "IDName": "", "Certificate": "111", "CertificateNo": "", "Capture_Time": "2019-03-02T18:56:08.000Z", "InstDateTime": "2019-03-02T18:56:27.000Z", "SeatIp": "", "SeatNo": "", "ID": "39195AI203", "LabelNub": "", "Terminal_Mac": "", "Terminal_Mac_terms": "", "URL": "http://cf.qq.com/act/a20180408ingame/other.htm", "url_terms": "cf.qq.com", "Title": "http://cf.qq.com/act/a20180408ingame/other.htm", "Longitude": "120.146646", "Latitude": "33.371189", "Device_Num": "th0200", "Device_Mac": "", "Device_Mac_terms": "", "Site_Code": "th0200", "site_code_terms": "th0200", "Site_Name": "新苹果网吧", "Area": "0001", "PoliceStation": "1001", "OrgCode": "55080760X", "TypeID": 1, "address": "盐南西路4号", "device_class": "", "PersonType": [], "PersonNo": "0", "Source": "120", "systemtime": "2019-03-02T19:15:41.000Z"}}, {"_index": "url_2", "type": "url", "id": "228d2653-321f-4d0f-b4cd-6cf48c0cb96a", "score": 1, "source": {"unitstype": "0", "Auth_Type": "1021111", "Auth_Account": "", "Session_ID": "F5A3ABDCFB794A04BA14A28C1A5F7AD8", "IDName": "", "Certificate": "111", "CertificateNo": "", "Capture_Time": "2019-03-02T18:55:08.000Z", "InstDateTime": "2019-03-02T18:56:28.000Z", "SeatIp": "", "SeatNo": "", "ID": "389874I801", "LabelNub": "", "Terminal_Mac": "", "Terminal_Mac_terms": "", "URL": "http://cache.tv.qq.com/win/play.html?cid=sifd2an7kx2h9h8&vid=u0842hewkzv", "url_terms": "cache.tv.qq.com", "Title": "http://cache.tv.qq.com/win/play.html?cid=sifd2an7kx2h9h8&vid=u0842hewkzv", "Longitude": "120.052235", "Latitude": "33.367367", "Device_Num": "YD079", "Device_Mac": "", "Device_Mac_terms": "", "Site_Code": "YD079", "site_code_terms": "YD079", "Site_Name": "龙腾网吧", "Area": "0010", "PoliceStation": "0106", "OrgCode": "55080760X", "TypeID": 1, "address": "", "device_class": "", "PersonType": [], "PersonNo": "0", "Source": "120", "systemtime": "2019-03-02T19:15:41.000Z"}}, {"_index": "url_3", "type": "url", "id": "2895226d-5033-46fa-90d8-70bb1faa0d55", "score": 1, "source": {"unitstype": "0", "Auth_Type": "1021111", "Auth_Account": "", "Session_ID": "F217D43EA1E74B3C9DF633B9F850E908", "IDName": "", "Certificate": "111", "CertificateNo": "", "Capture_Time": "2019-03-02T18:55:20.000Z", "InstDateTime": "2019-03-02T18:56:28.000Z", "SeatIp": "", "SeatNo": "", "ID": "25196AQ351", "LabelNub": "", "Terminal_Mac": "", "Terminal_Mac_terms": "", "URL": "http://cache.tv.qq.com/pcbarrage/barragev2.html", "url_terms": "cache.tv.qq.com", "Title": "http://cache.tv.qq.com/pcbarrage/barragev2.html", "Longitude": "120.052235", "Latitude": "33.367367", "Device_Num": "YD079", "Device_Mac": "", "Device_Mac_terms": "", "Site_Code": "YD079", "site_code_terms": "YD079", "Site_Name": "龙腾网吧", "Area": "0010", "PoliceStation": "0106", "OrgCode": "55080760X", "TypeID": 1, "address": "", "device_class": "", "PersonType": [], "PersonNo": "0", "Source": "120", "systemtime": "2019-03-02T19:15:41.000Z"}}, {"_index": "url_4", "type": "url", "id": "9dc5006d-d6f8-4788-a40c-d630fa02fa74", "score": 1, "source": {"unitstype": "0", "Auth_Type": "1021111", "Auth_Account": "", "Session_ID": "8C71998E30604A639FA6DA27C594023B", "IDName": "", "Certificate": "111", "CertificateNo": "", "Capture_Time": "2019-03-02T18:55:56.000Z", "InstDateTime": "2019-03-02T18:56:28.000Z", "SeatIp": "", "SeatNo": "0013", "ID": "CB8908S341", "LabelNub": "", "Terminal_Mac": "", "Terminal_Mac_terms": "", "URL": "http://mg7800.com/", "url_terms": "mg7800.com", "Title": "http://mg7800.com/", "Longitude": "120.052235", "Latitude": "33.367367", "Device_Num": "YD079", "Device_Mac": "", "Device_Mac_terms": "", "Site_Code": "YD079", "site_code_terms": "YD079", "Site_Name": "龙腾网吧", "Area": "0010", "PoliceStation": "0106", "OrgCode": "55080760X", "TypeID": 1, "address": "龙岗居委会三组青龙华庄5幢", "device_class": "", "PersonType": [], "PersonNo": "0", "Source": "120", "systemtime": "2019-03-02T19:15:41.000Z"}}
```

## What happened in the past a 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.**

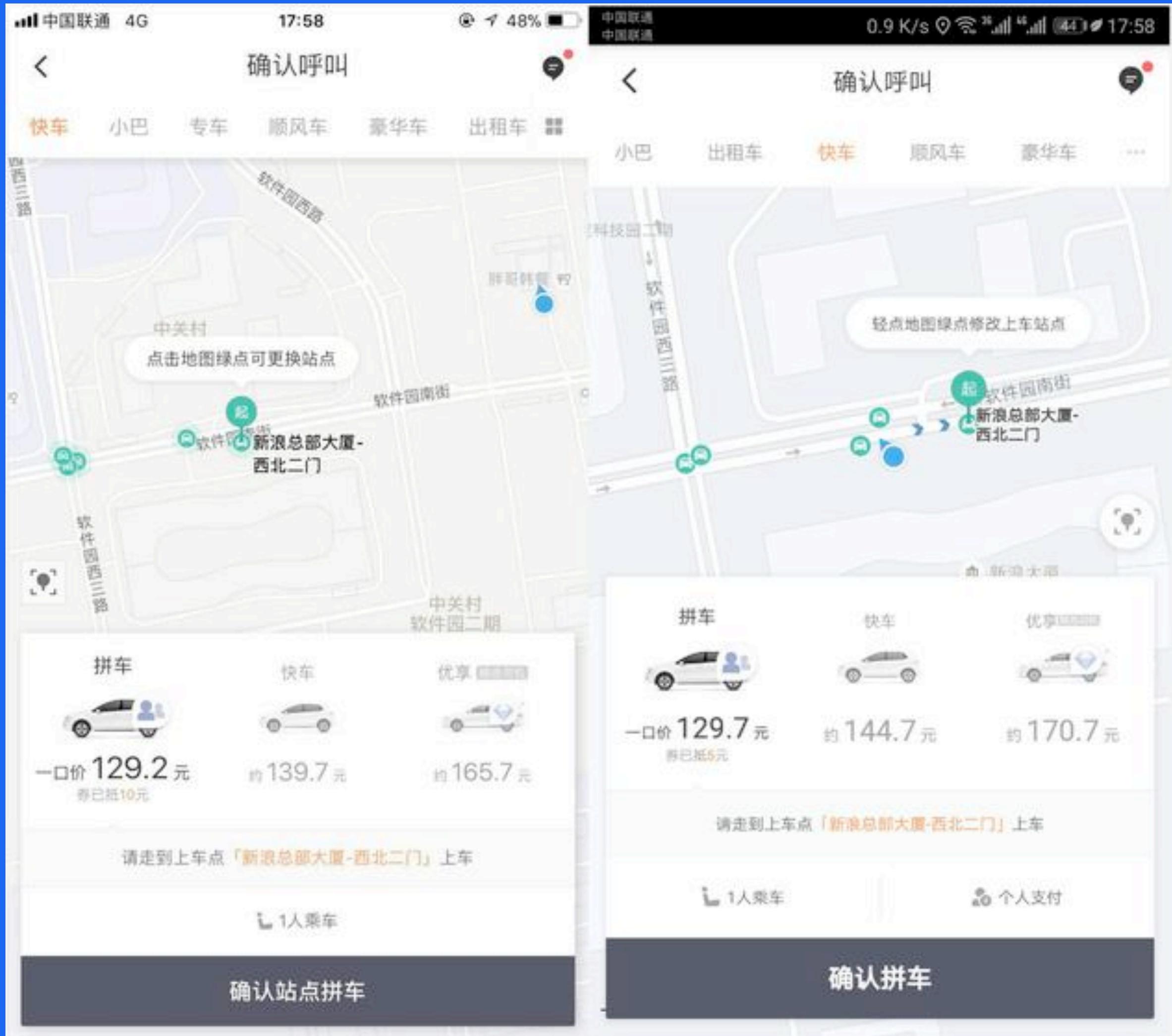
2:00 AM · Jun 2, 2019 · Twitter for iPhone

---

**13.1K Retweets    48.6K Likes**

CHINESE CONSUMERS FAVOR EFFICIENCY  
AT THE EXPENSE OF PRIVACY  
- ROBIN LI, CEO OF BAIDU





Didi, Chinese Uber



Ctrip, Chinese Expedia

## 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

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

## **2. What is identity?**

## BY DEFINITION

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

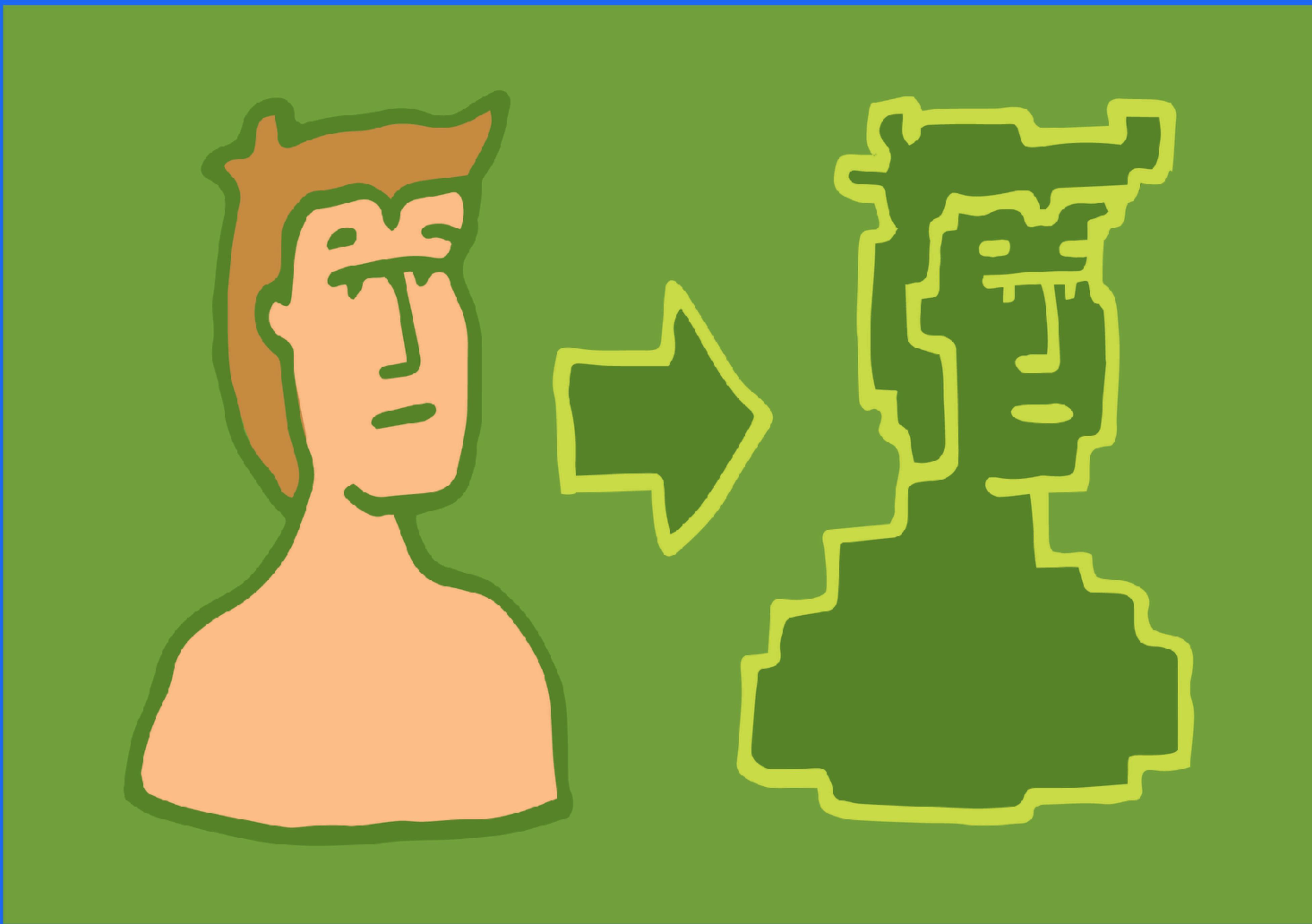


*"Which one of us is me?"*

(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

f t  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

Search 1Password + Edit

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

58 items sorted by Title ▾

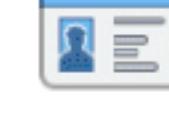
A

-  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

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

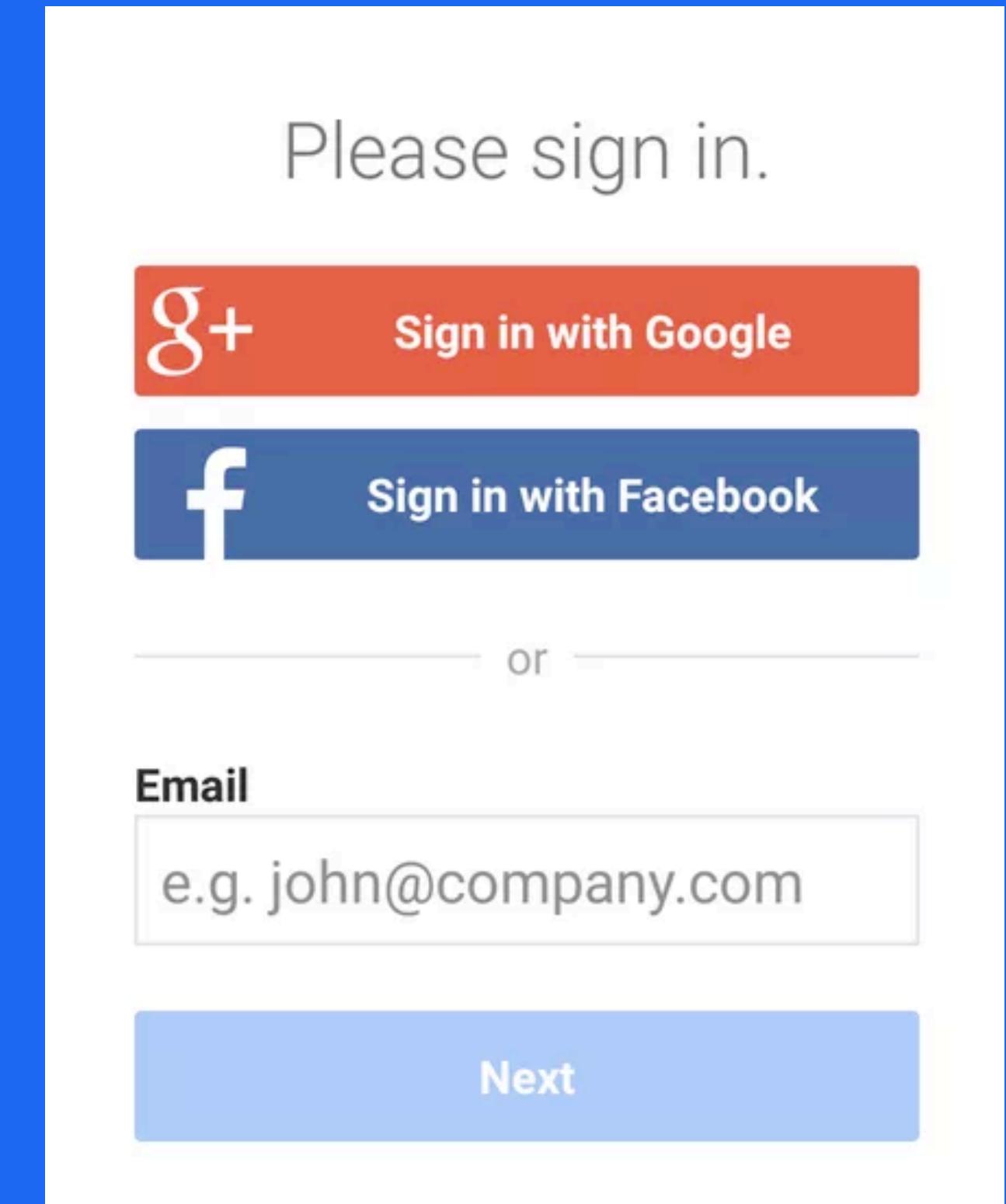
[View Saved Form Details](#)

## 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
- ▶ Decentralized 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 an 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?

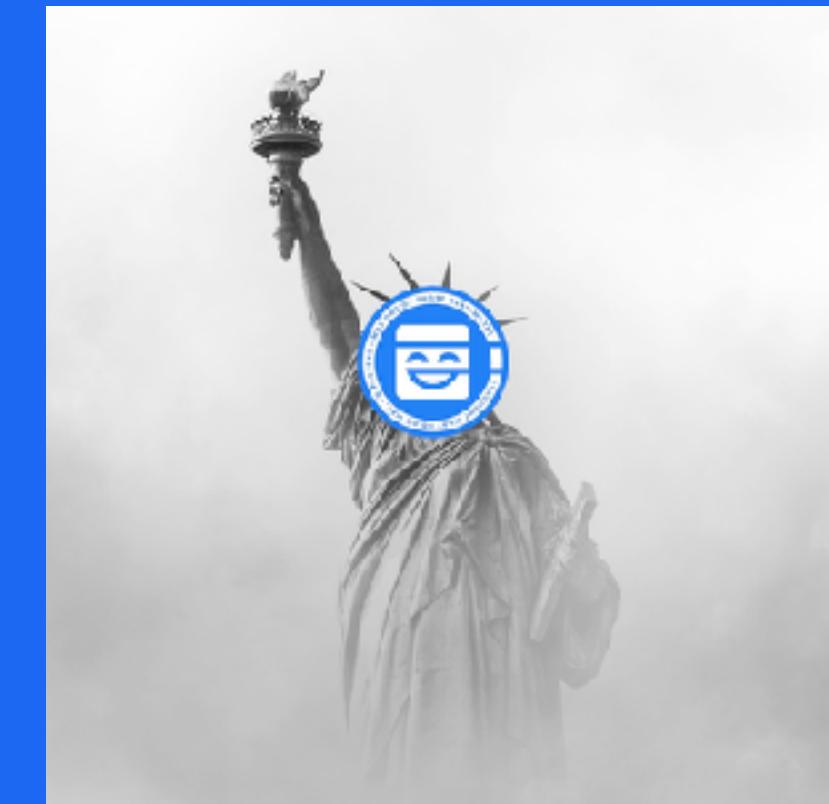
WE CAN, BUT NOT EVERYONE

## 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

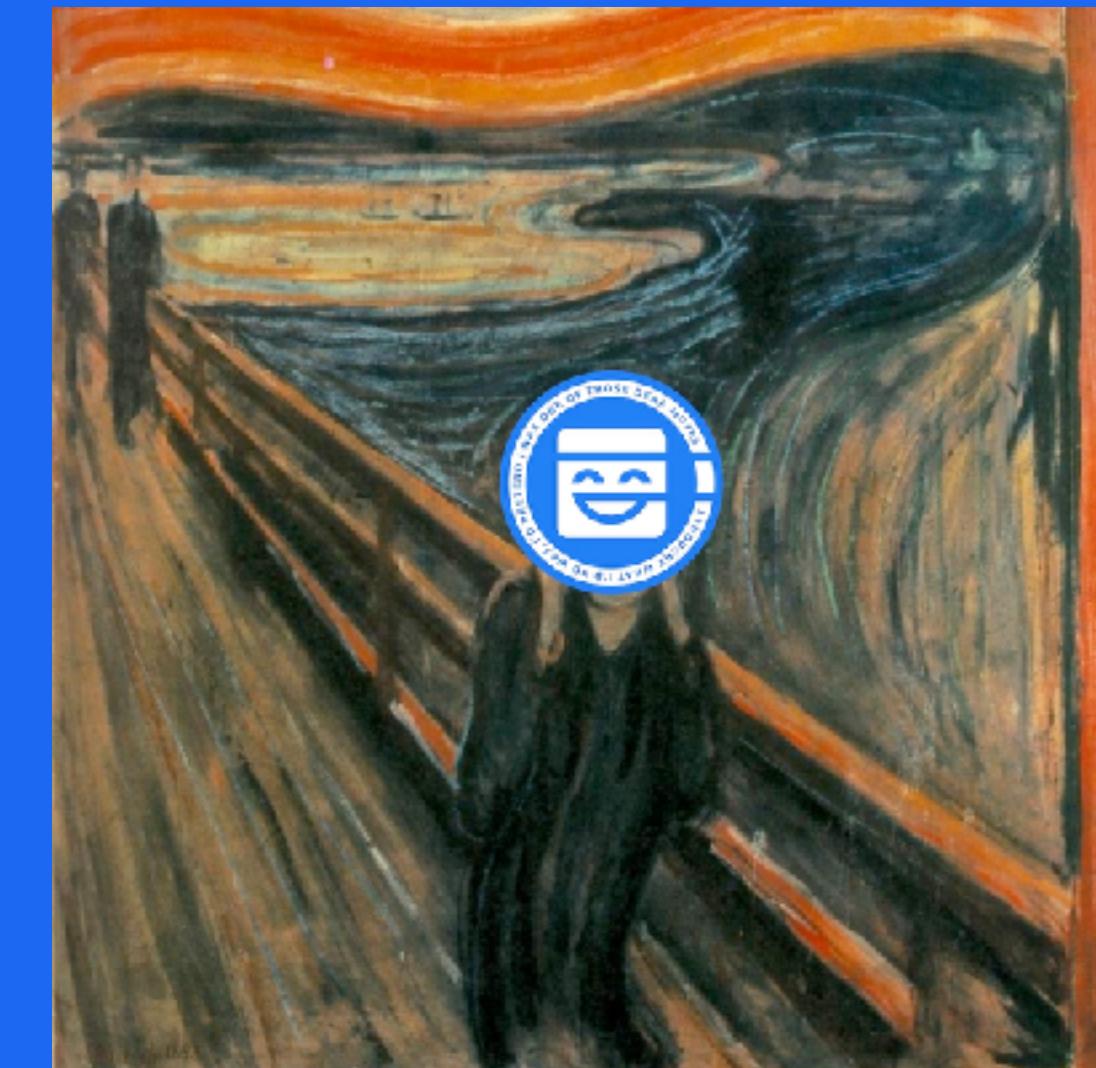
# Maskbook

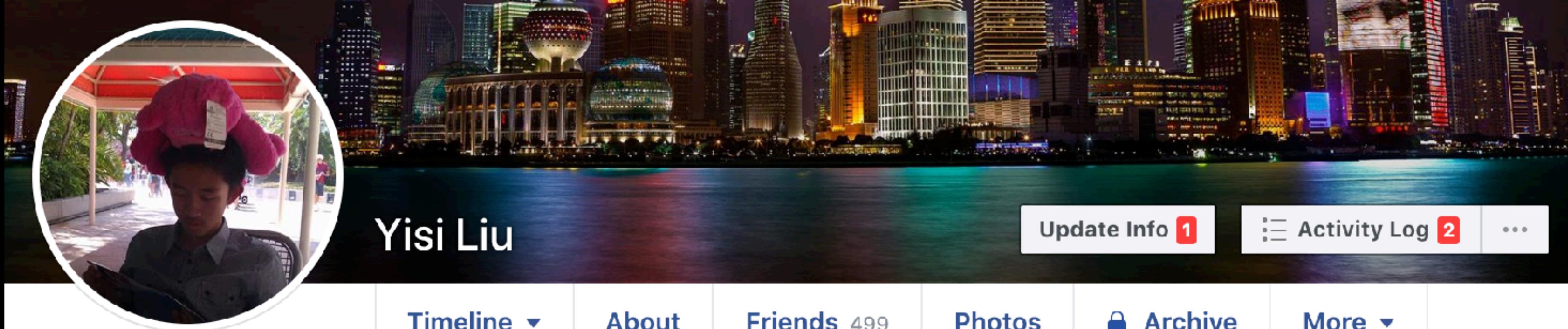
- ▶ What is Maskbook?
- ▶ A browser extension
- ▶ Each user with an unified identity (secp256k1 key pair) and link it to their Facebook account
- ▶ Create encrypted posts that only designated friends can decrypt
- ▶ Hide from no one but Facebook



## 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

A8cEYX3FvuU8HmpDrtrxFKFHdTLn505gT2t7JdMj  
HDu5K 

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?



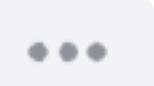
Photo/Video



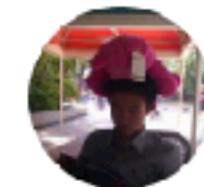
Tag Friends



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:

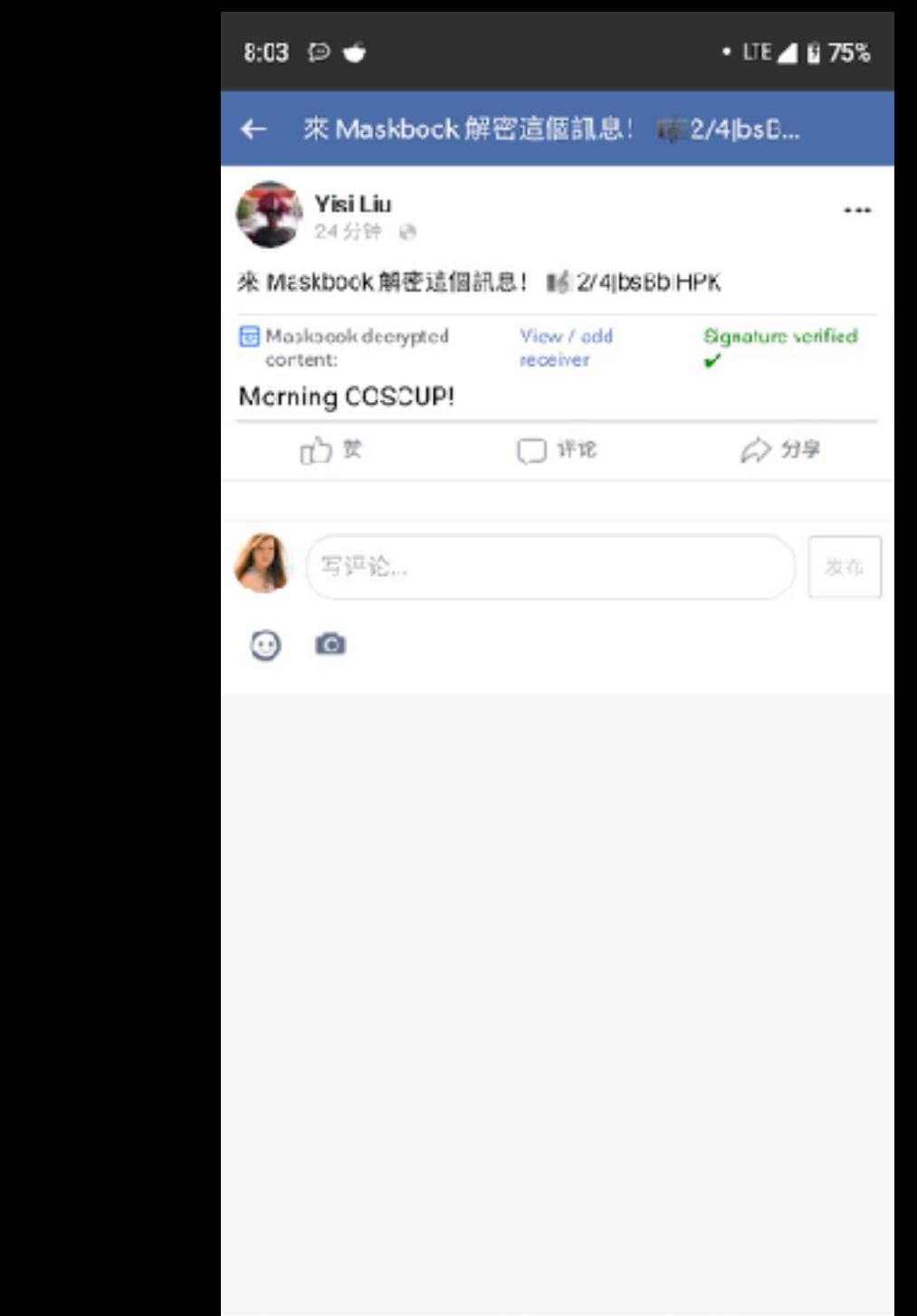
查看或添加收件人 數字簽名驗證成功 ✓

Morning COSCUP!

Like

Comment

Share



Create Post

What's on your mind, Yisi?

Photo/Video Tag Friends Feeling/Activ... News Feed Your Story

Post

Encrypt with Maskbook

有何所思? 用 Maskbook 加密分享。

鍵入以搜尋

選取全部

1 100000175076210 5+hxuzopohldfp/0ncwiapl5mc3+cqgznrjjf7v4=

Лариса Харитонова hxsug2q+jyc81ch0uqxutlet0qrg20f2oe3cp5q5szw=

andrew.tu3 wwmewgizabendboqy4f5ganuwknscd6efzq1sjalfau=

Эля Домерщикова heufbxrz4tgyyvddn6plukm+xa5ifjdvcc2q+ugyt8=

Neruthes de Neoparia gdg5vsee511f7pwtejaord/4e3j6frdpxjdhnylyga=

Create Post

What's on your mind, Yisi?

Photo/Video Tag Friends Feeling/Activ... News Feed Your Story

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/SclU5htwMtmriBYzFNvzHfmahwOmesnVfcEZNdq7krnaGh9Q7is/6rp6HlyMBQr481aEjhADmyTGckNyCqlKyIP/KYcP209/2kLFbKK4a5kpqt4Jxcxv7eex5e5Obrwpsm8NnwKHvn67D928eEqYlqtAlwUwHjlcfQWS6TUYLjF8nuTh38neNmi0jg3dl3Q==|TTjbqWenmhEyKL1C2uJdAUOTNE4yAUf3UmpXMBvJQQ==|TxXcljBYppukqz38jg1025RhrnrAvsb+PZ9bT9zSiTtzFwYYp91N0PJFvnP1RJhAarCzimXEx1ljn+OrRpStA==||

Photo/Video Tag Friends Feeling/Activ... News Feed Your Story

Post

Encrypt with Maskbook

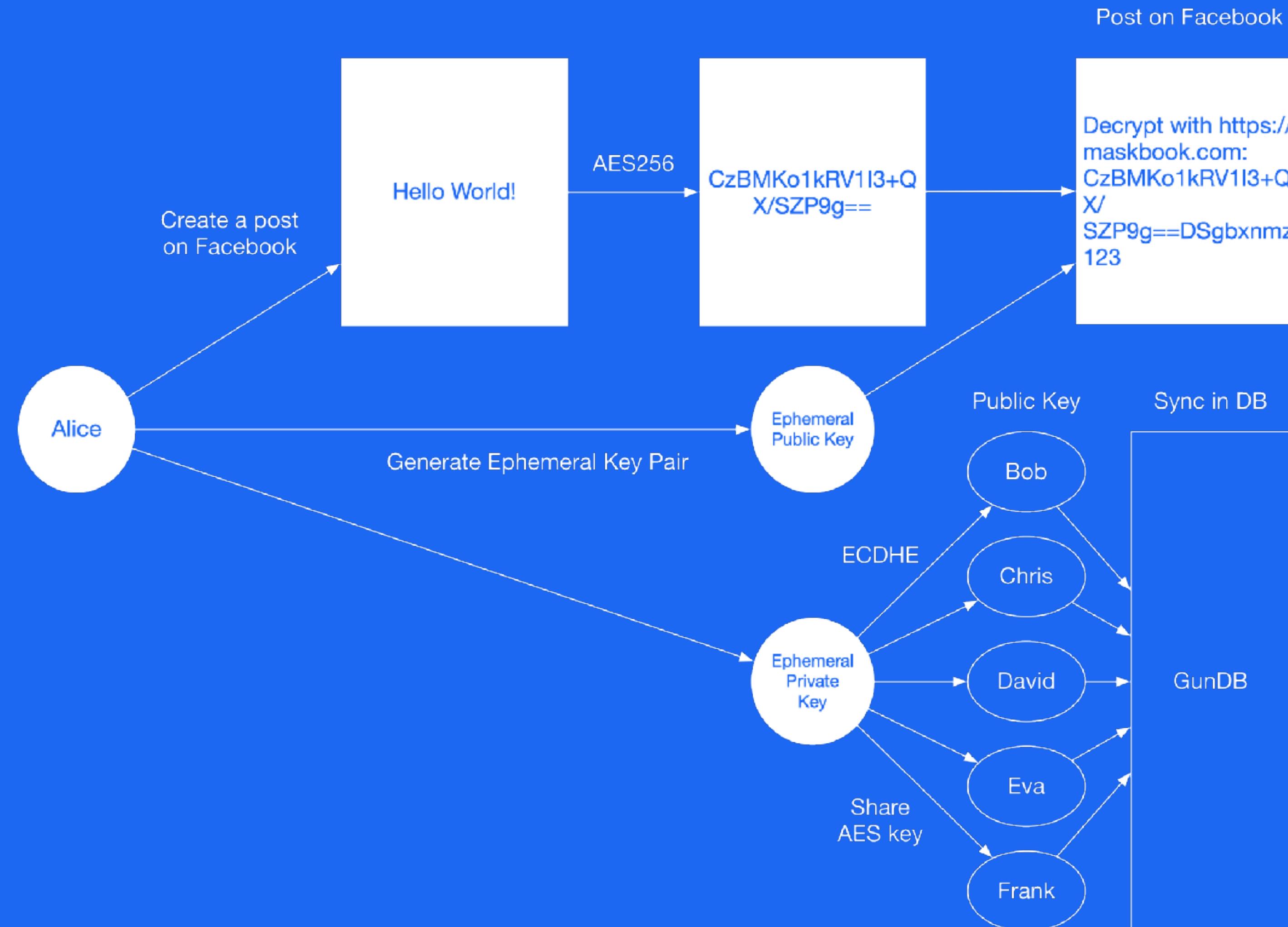
Morning COSCUP!

100000175076210 × Лариса Харитонova ×  
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!

# Maskbook Architecture

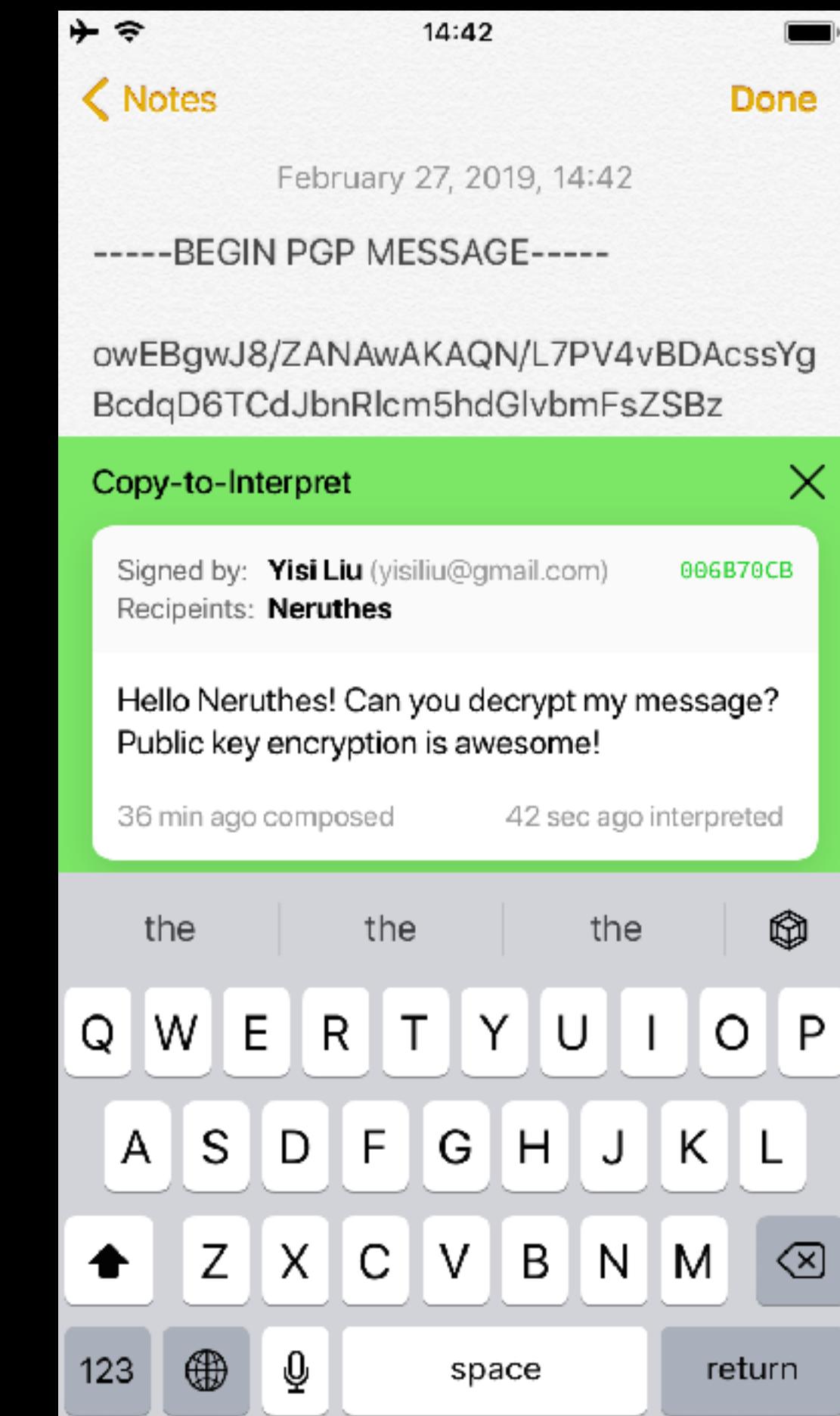
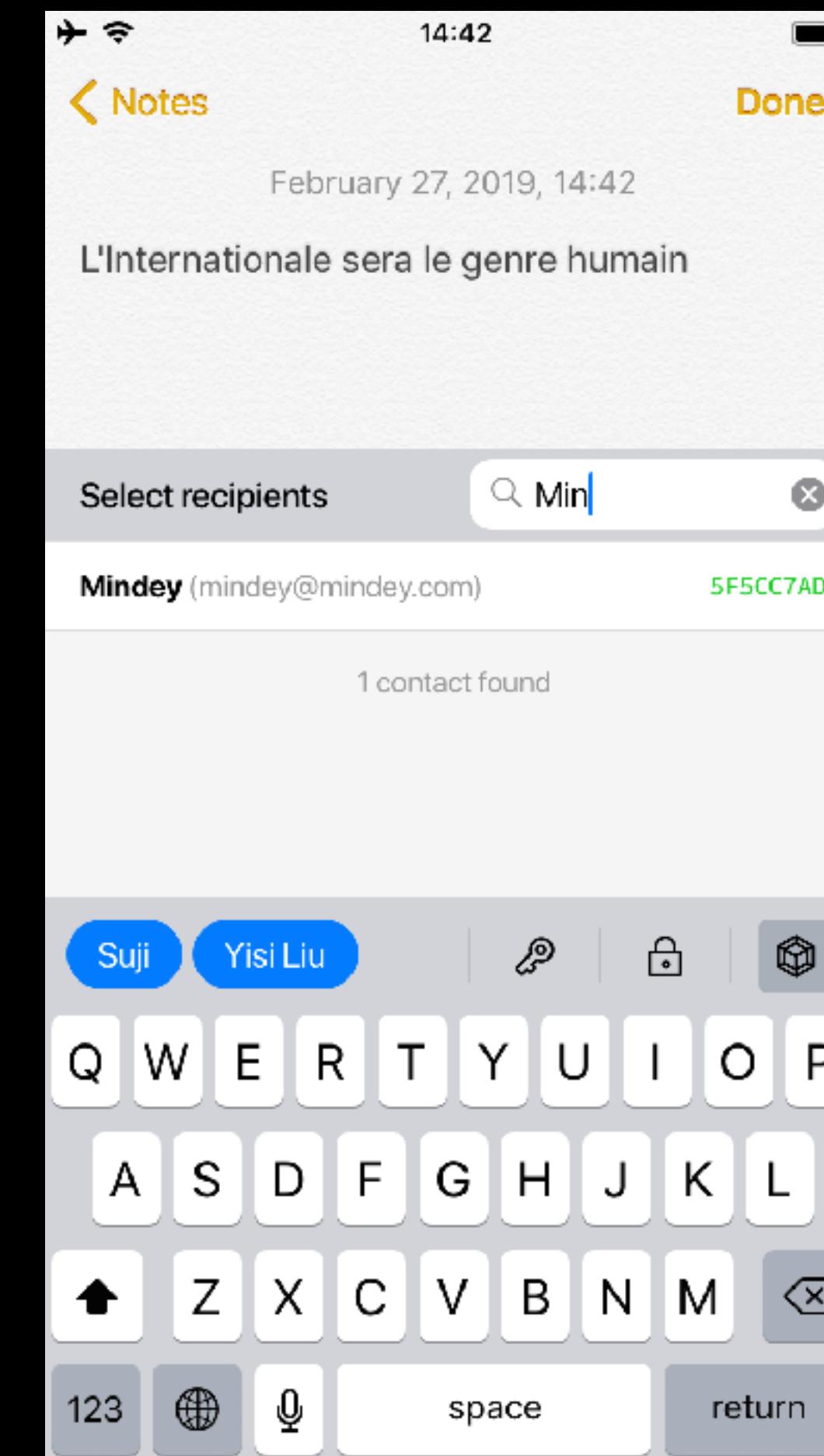
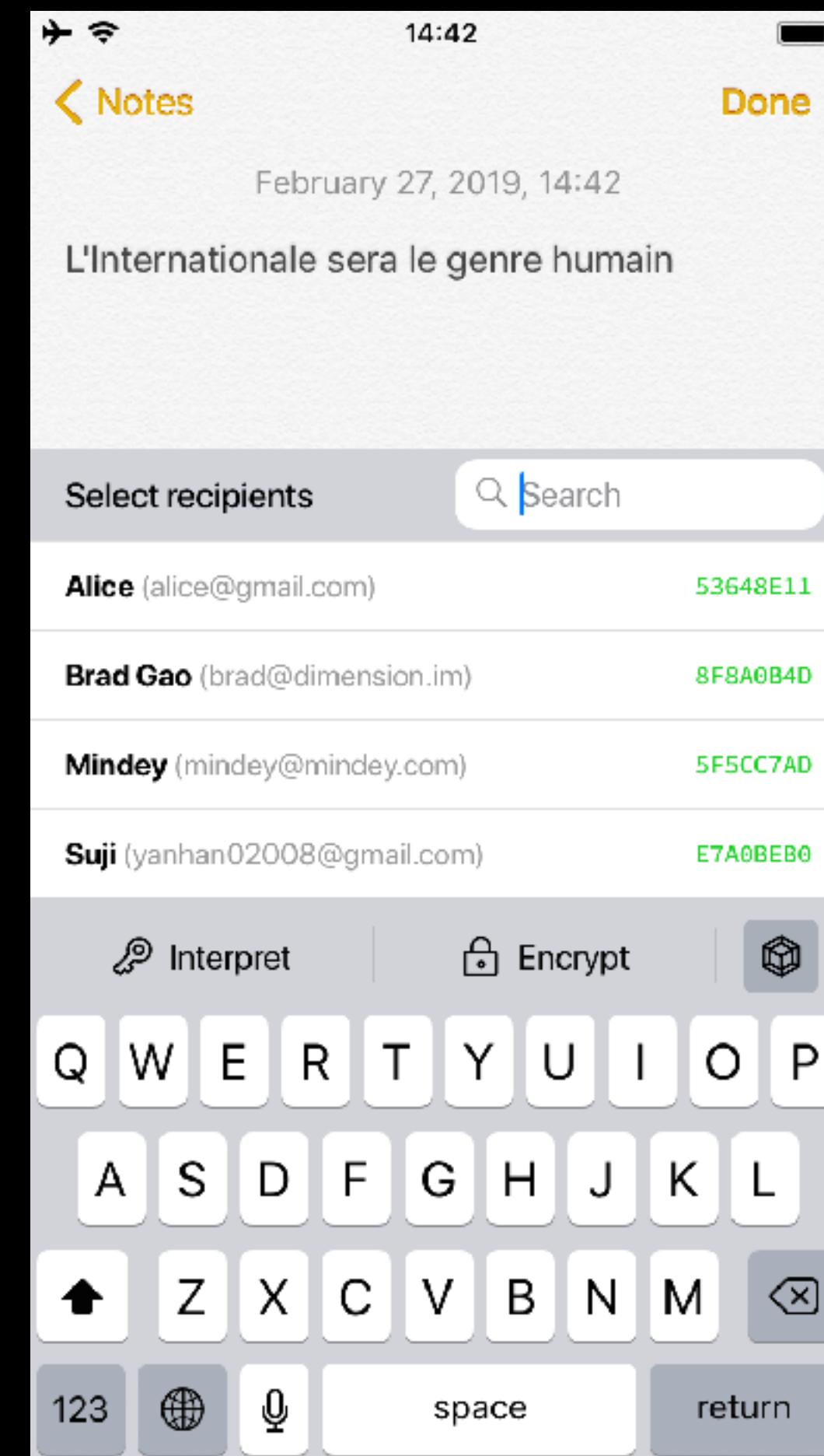
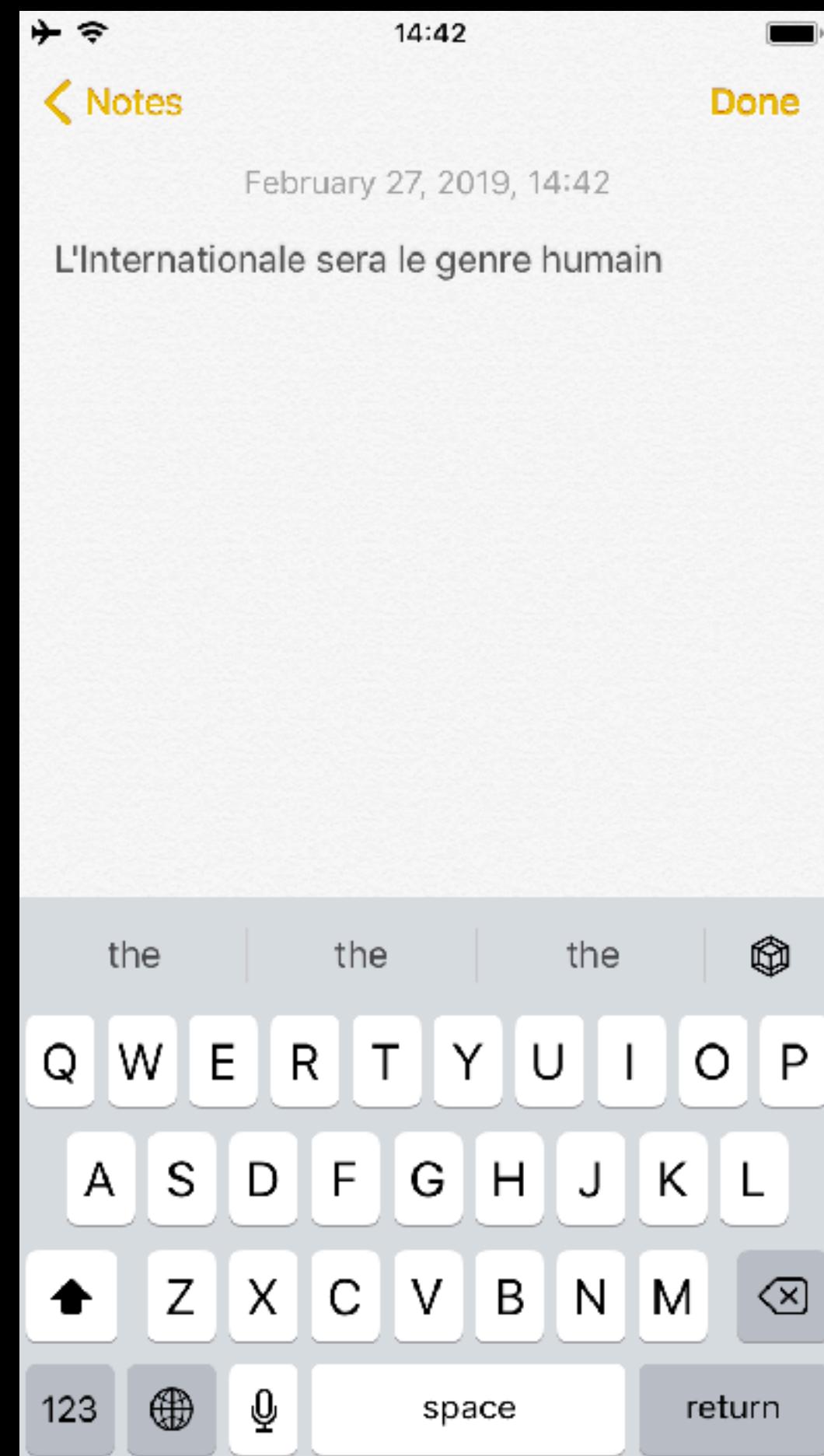


## Tessercube

- ▶ 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



Comparison	Allo	iMessage	Messenger	Riot	Signal	Skype	Telegram	Threema	Viber	Whatsapp	Wickr	Wire
<b>TL;DR: Does the app secure my messages and attachments?</b>	No	No	No	No	Yes	No	No	Yes	No	No	No	Yes
<b>Company jurisdiction</b>	USA	USA	USA	UK	USA	USA	USA / UK / Belize	Switzerland	Luxembourg / Japan	USA	USA	Switzerland
<b>Infrastructure jurisdiction</b>	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
<b>Implicated in giving customers' data to intelligence agencies?</b>	Yes	Yes	Yes	No	No	Yes	No	No	No	Yes	No	No
<b>Surveillance capability built into the app?</b>	No	No	No	No	No	Yes	No	No	No	No	No	No
<b>Does the company provide a transparency report?</b>	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes
<b>Company's general stance on customers' privacy</b>	Poor	Poor	Poor	Good	Good	Poor	Poor	Good	Poor	Poor	Good	Good
<b>Funding</b>	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
<b>Company collects customers' data?</b>	Yes	Yes	Yes	No	No	Yes	Yes	No	Yes	Yes	No	No
<b>App collects customers' data?</b>	Yes	Yes	Yes	Minimal	Minimal	Yes	Yes	No	Yes	Yes	No	Minimal

## 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, Telegram
- ▶ 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



FIND US ON

MASKBOOK.COM

TESSERCUBE.COM