Enhanced Privacy with Decentralized Identity

Yisi Liu

DIMENSION

What Is Privacy?

- A fundament right that is essential to autonomy and the protection of human dignity
- Many other human rights are built upon privacy
- Privacy helps us create boundaries to limit who has access to our bodies, places or things
- Privacy ensures that we are not controlled or influenced by unwanted people or parties

Are our privacies compromised?

YES!

Are our privacies compromised?

Are our privacies compromised?

- 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”

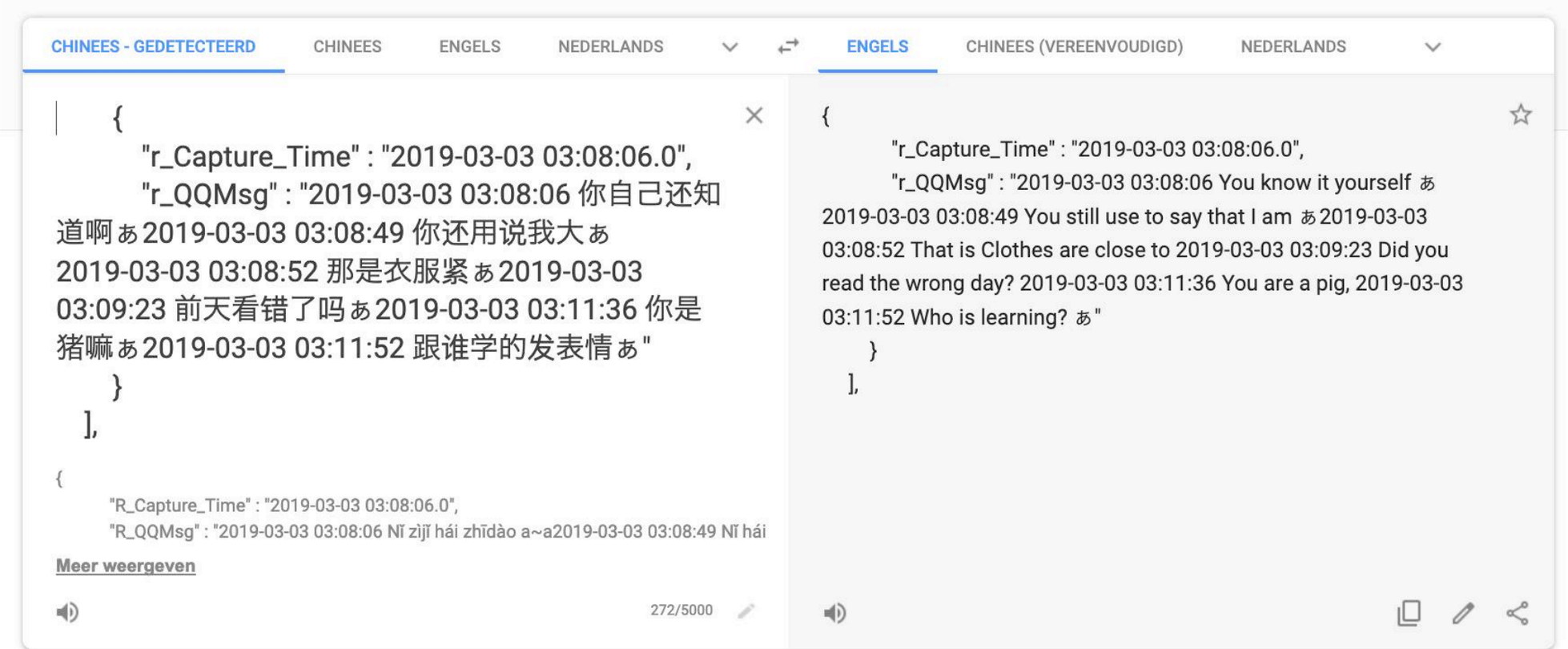
Are our privacies compromised?

- Facebook–Cambridge Analytica data scandal
- 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

Are our privacies compromised?

- Facebook–Cambridge Analytica Data Scandal
- Equifax Data Breach
- WeChat Data Breach

Are our privacies compromised?



Source: Victor Gevers

Are our privacies compromised?

- Facebook–Cambridge Analytica Data Scandal
- Equifax Data Breach
- WeChat Data Breach
  - Over ~1 billion users are affected
  - Over 300m Chinese private messages are exposed
  - The government is reported monitoring through both social media and instant messaging, not just in China

Are our privacies compromised?

- Facebook–Cambridge Analytica Data Scandal
- Equifax Data Breach
- WeChat Data Breach
- Tianyan and Prism Surveillance Program

Why Is This Important?

- We are under surveillance without being notified
- Our data is collected and shared across platform
- One can be easily profiled and identified only with arbitrary data points
- Unlike other rights being violated, your privacy can be compromised without making you aware

What Has Been Done

- General Data Protection Regulation (GDPR) in Europe
  - Privacy by design
  - No personal data is allowed to be stored 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

"Many companies have decided to put compliance with the GDPR as one of their key tasks on management level. Some major players are even changing their strategies in order to become leaders regarding data protection friendly products and services."

–Jan Philipp Albrecht

What Is Identity?

- "**Identity** is the qualities, beliefs, personality, looks and/or expressions that make a person or group."

- The social identity is how you look like in the society
  - Your name
  - Your gender
  - Your nationality
  - Your occupation
  - Verified by the government

"Which one of us is me?"

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

What Is Identity?

- “**Identity** is the qualities, beliefs, personality, looks and/or expressions that make a person or group.”

- The social identity is how you look like in the society

- The digital identity is how you look like on the Internet

    - Your Facebook account

    - Your Google account

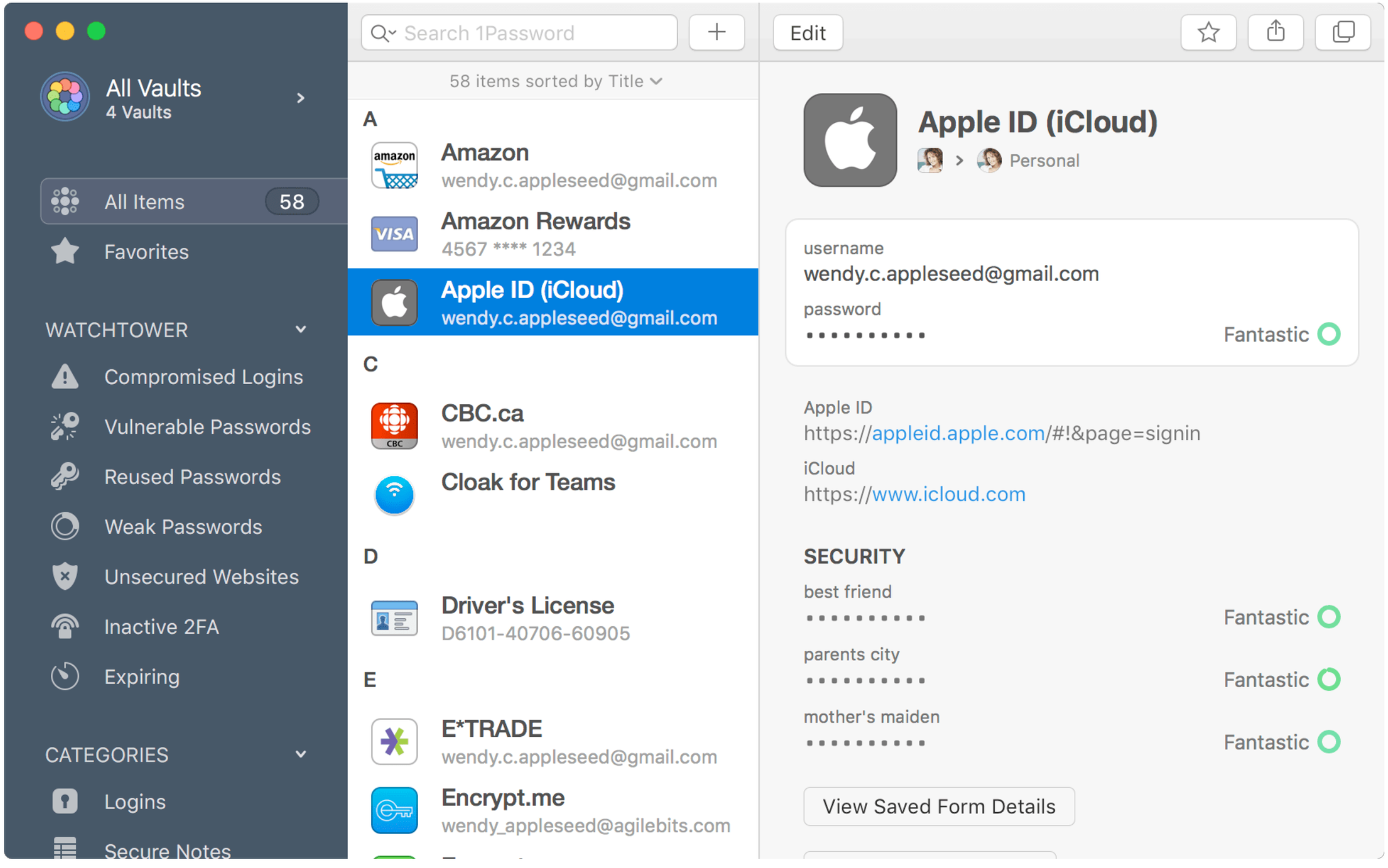
    - Your Reddit account

    - Verified by third-party organizations

Current Problems with Digital Identities

- 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…

Current Solutions

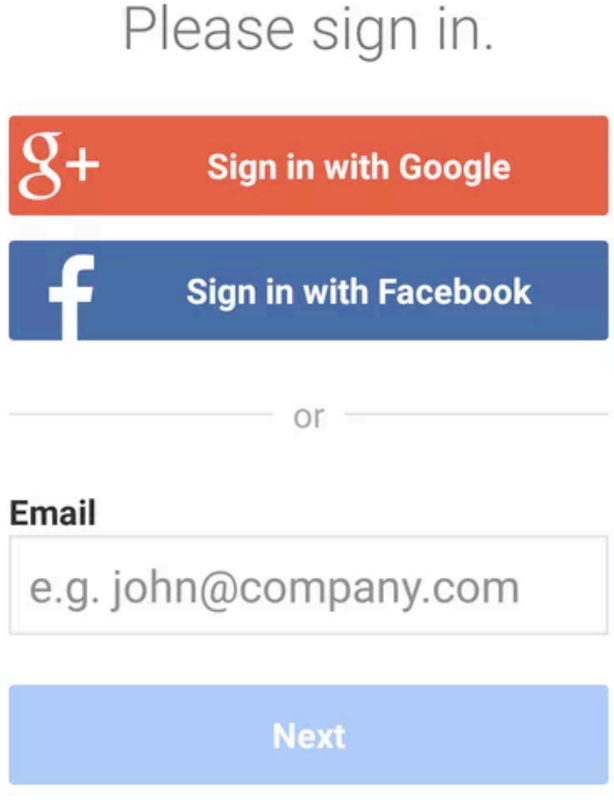


Current Solutions

- Password Management Tools, e.g. 1 Password, LastPass
- OpenID, e.g. Google Login, Facebook Login
- Unified identity/identifier
- Single Sign On (SSO) so users only need to login once
- Trust dependent on the Identity Provider (IdP)
- Vulnerable to multiple attacks due to its low level security design

Current Solutions

- Password Management Tools, e.g. 1 Password, LastPass
- OpenID, e.g. Google Login, Facebook Login



Current Solutions

- Password Management Tools, e.g. 1 Password, LastPass
- OpenID, e.g. Google Login, Facebook Login
- Decentralized Identity

Decentralized Identity

- A digital Identity created by the user themselves
- Can be verified without a third party
- Can gain enough trust to prove the identity
- Users can decide which part of their information to share with the different organizations
- Users own and control their data

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 is the trust?

- Blockchain, or more generally, distributed ledger technology (DLT)

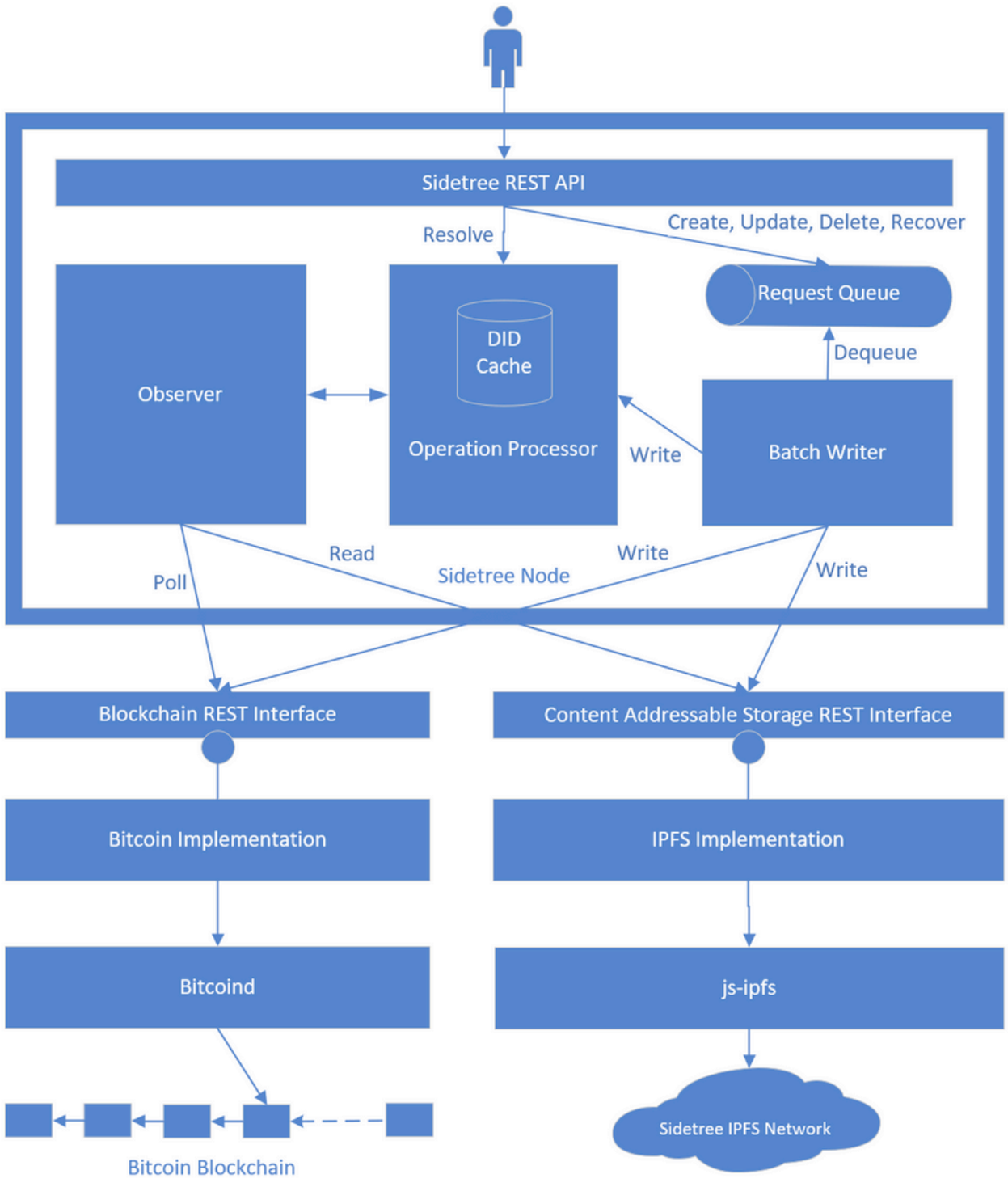
- Each identity is stored on DLTs

- 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

Identity Overlay Network



Then, where is 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 problems

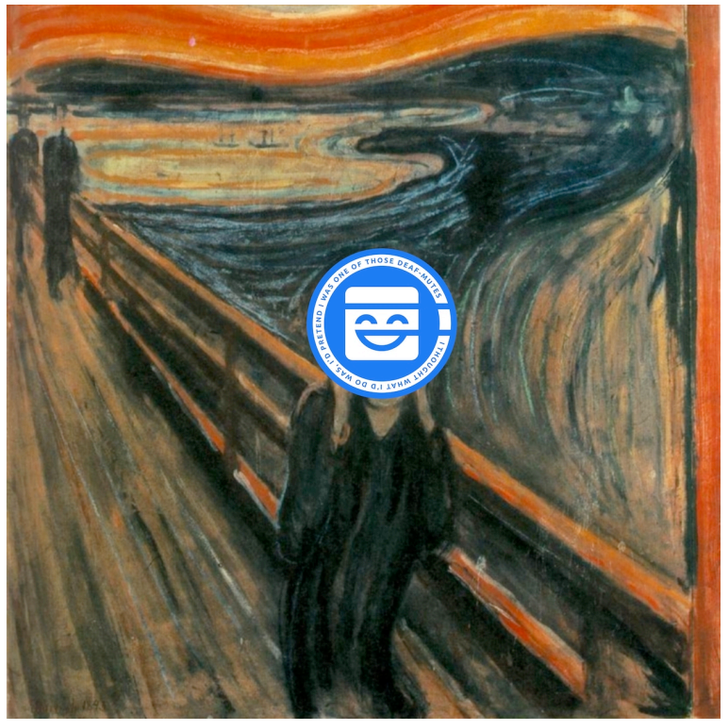
Privacy-Ensured Solutions

- 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 web 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

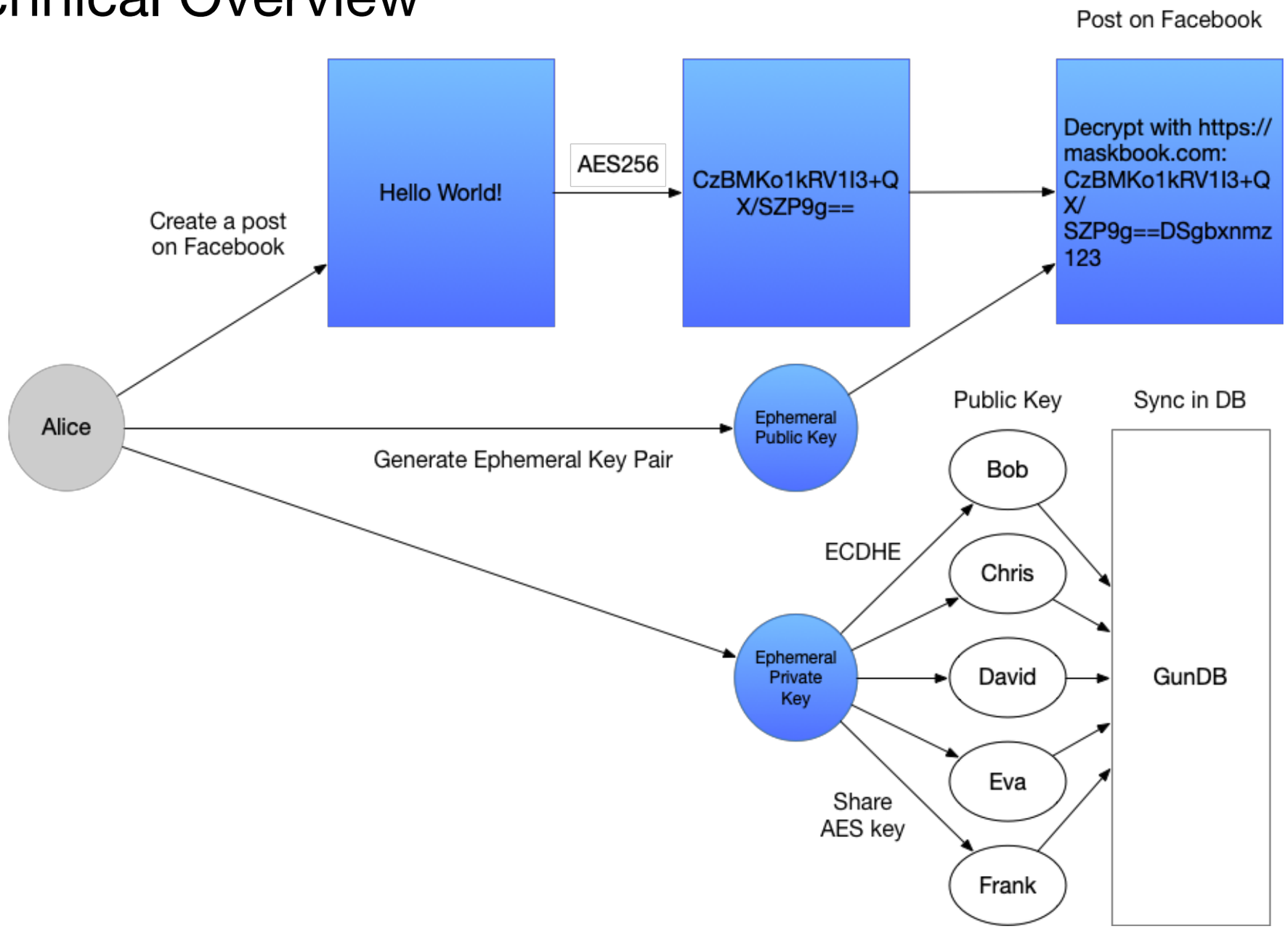
Maskbook



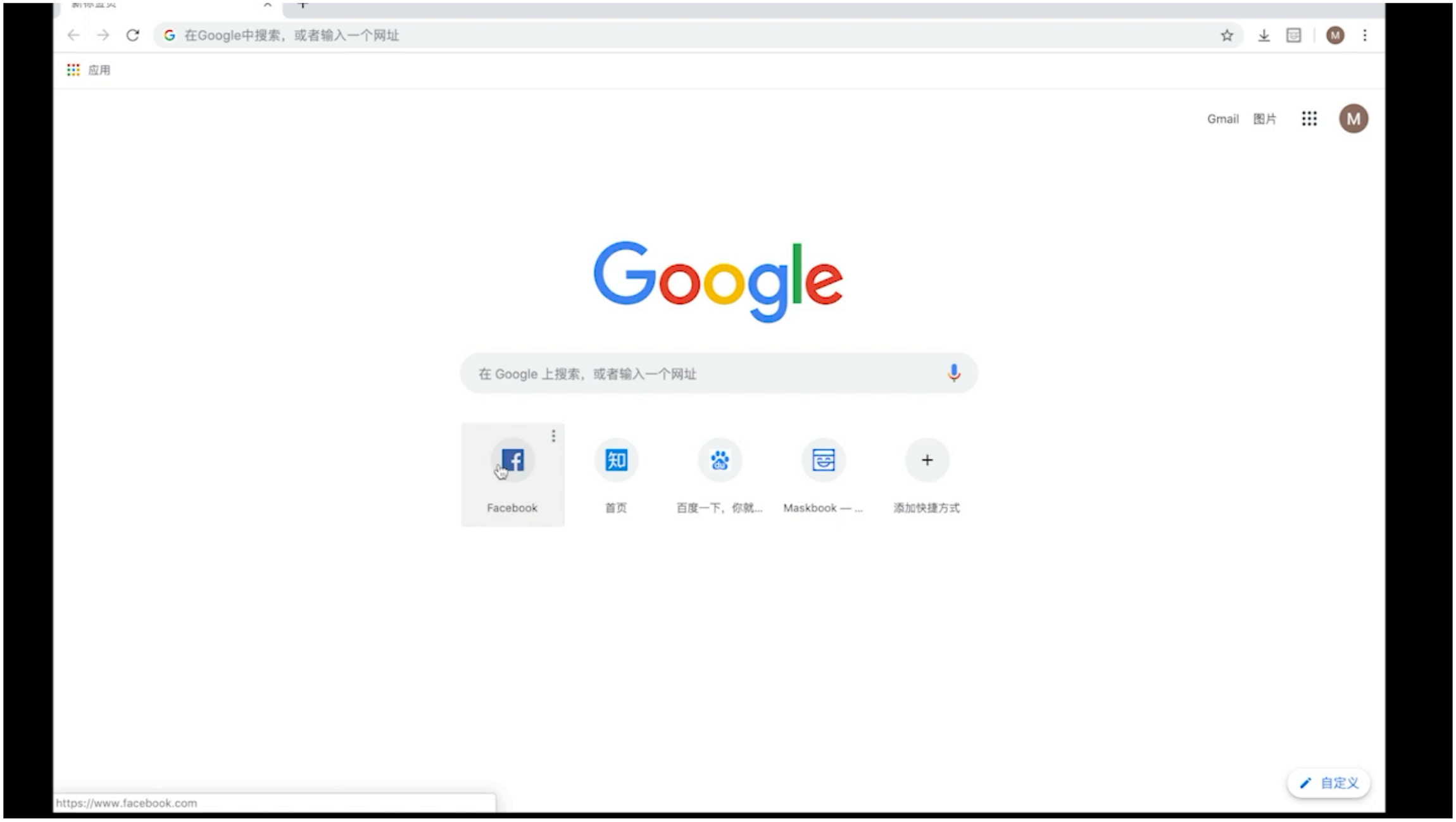
- Why Maskbook?
- We might have nothing to hide.
- But we also have nothing to surrender.
- And they must have nothing to steal.

Maskbook

- Technical Overview

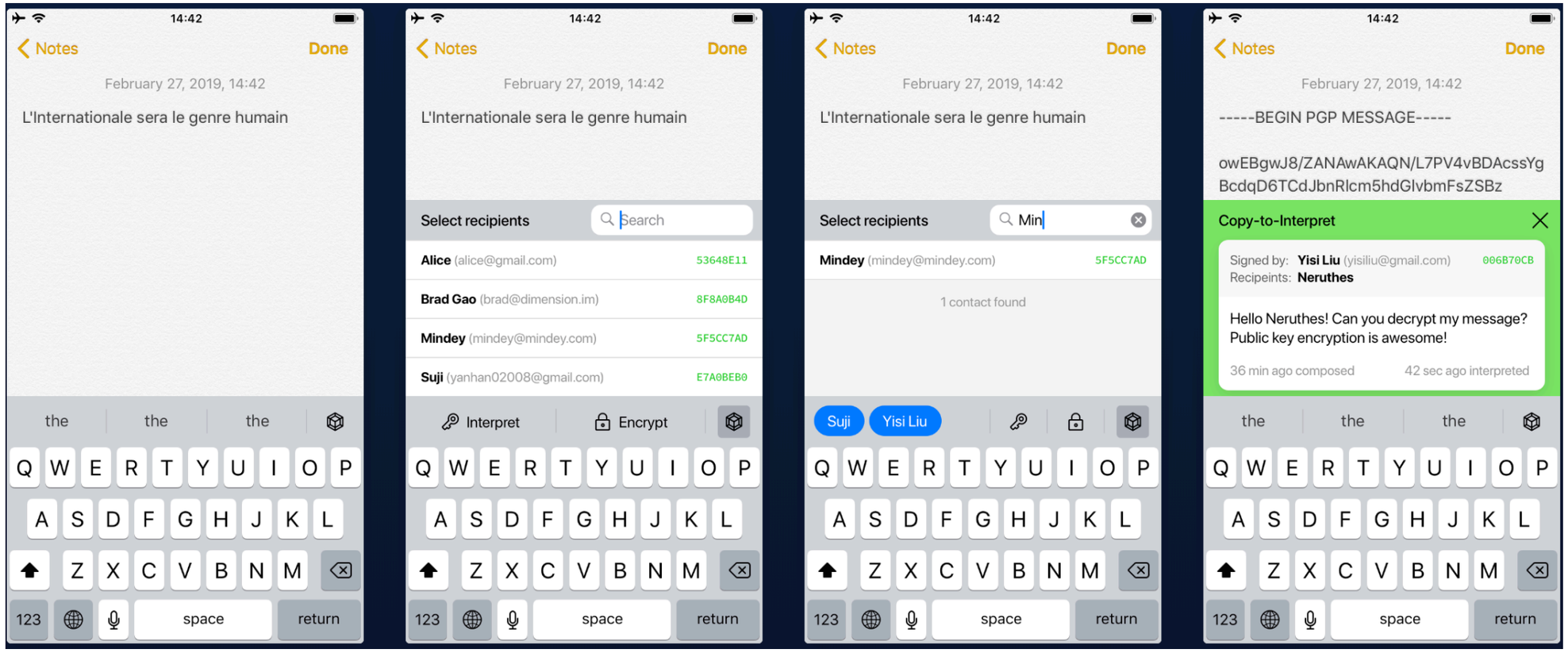


Maskbook


在Google中搜索，或者输入一个网址
应用
Gmail
图片
M
Google
在 Google 上搜索，或者输入一个网址
Facebook
首页
百度一下，你就...
Maskbook — ...
添加快捷方式
自定义
https://www.facebook.com

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

SECURE MESSAGING APPS COMPARISON

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)
  - Users would still need to use SECP256K1 key pair as their main identity
  - ECC has shorter keys and smaller payload size than RSA

Decentralized Identity

- The key pair is apart from the accounts the user is using
- One can use the same key pair to participate in all supported services or products
- Forms a new identity network

Is this really what we want?

- Encrypt everything we are sending and viewing
- Protect against anyone we don’t want to share with
- Is there something missing?

Crypto-Anarchism

Crypto anarchy will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

--*The Crypto Anarchist Manifesto*
Timothy C. May, 1988

Crypto-Anarchism

- It is not real “anarchy”
- “Crypto-anarchists employ cryptographic software to evade persecution and harassment while sending and receiving information over computer networks, in an effort to protect their privacy, their political freedom, and their economic freedom.”

Trade-off between Privacy and Security

- Tor Project is adopted by a lot of terrorists, criminals and hides millions of “bad” things

- Bitcoin and later developed Monero are largely adopted and used in Dark Web transactions

- There is a trade-off between privacy and (global) security

Solutions towards the Balance

- We don’t want our products to further help those terrorists and criminals against the global security

- Metadata is still remained accessible by service providers and even the government per request

- We are working on a zero-knowledge sensor for dangerous contents

- Still remained in question

Future...

Thanks!

Check our websites at:

dimension.im
maskbook.com
tessercube.com

DIMENSION