Encrypted Email
How Hard Could It Be?

Dr. Andy Yen

CEO, Proton Technologies AG

ProtonMail

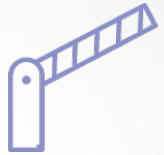
WHY EMAIL IS **GREAT**

The most democratic communication protocol in history.

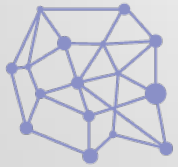
Everyone has one, everyone needs one

Original and most common digital identity

Free to send, and can send to anyone



Almost zero barrier to entry (mixed blessing)



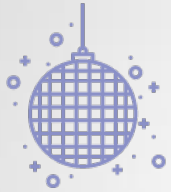
Decentralized (in principle)

Existing infrastructure, applications, & tools

Archiving

ProtonMail

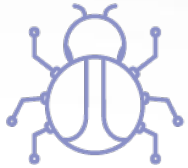
WHY EMAIL IS **AWFUL**



Protocols from the 80s and 90s (SMTP is from 1982)

RFC

Dozens of RFCs (not always followed)



Compatibility with tools/ applications/ message histories

- Parsing
- Encoding

Insecure (e-postcard)

Spam

ProtonMail

WHY END-TO-END ENCRYPT?

- Your **data is valuable** to
  - Governments
  - Companies
  - Criminals
- STARTTLS **will not save you**
- Database breaches are **when, not if**
- Purely legal protections **do not work**
- **Without privacy, democracy dies**

ProtonMail

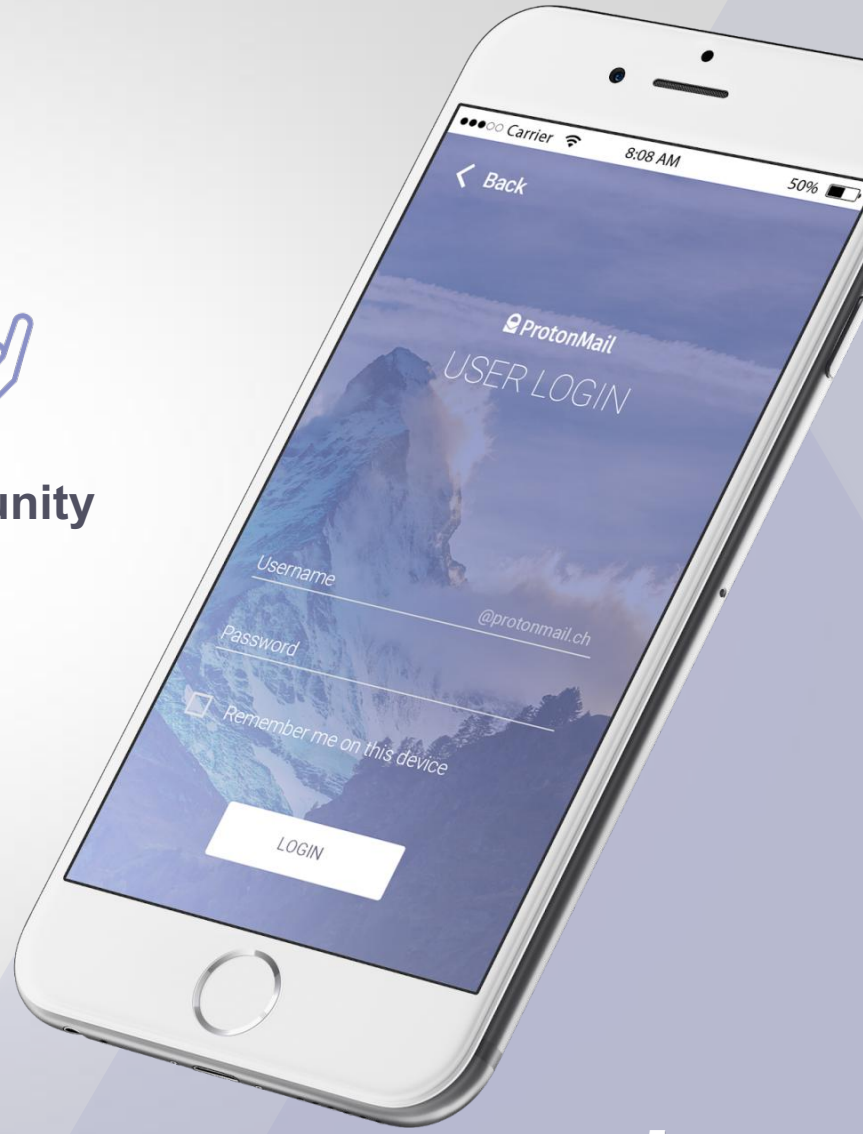
ProtonMail

World's largest encrypted email provider

Largest Swiss email provider

Open standards and open source

Community backed



OUR **MISSION** IS TO CREATE A
MORE SECURE AND **FREE INTERNET**

ProtonMail

“WE NEED TO **BUILD AN INTERNET** WHERE **PRIVACY** IS **NO LONGER JUST AN OPTION**, BUT THE **DEFAULT**.”

SECURE BY DESIGN PRINCIPLES

- **UX matters** — if nobody uses it, it does not matter if it is secure
- Do not invent your own **cryptography**
- No security theater, but **security is an onion** — layered is good
- Trade-offs are inevitable, but **make the right trade-offs**
- Define threat models and **educate your users**
- You, the provider, should be part of a **threat model**

ProtonMail

HOW PROTONMAIL WORKS

CLIENT

- User interface
- Generates keys
- Encrypts/decrypts/verifies messages and attachments
- All content encrypted before upload to server

SERVER

- Access control
- Stores ciphertext and metadata
- Receives and encrypts mail if not encrypted already
- Delivers sent messages
- Public key infrastructure (PKI)

Under the hood, we implement **OpenPGP**

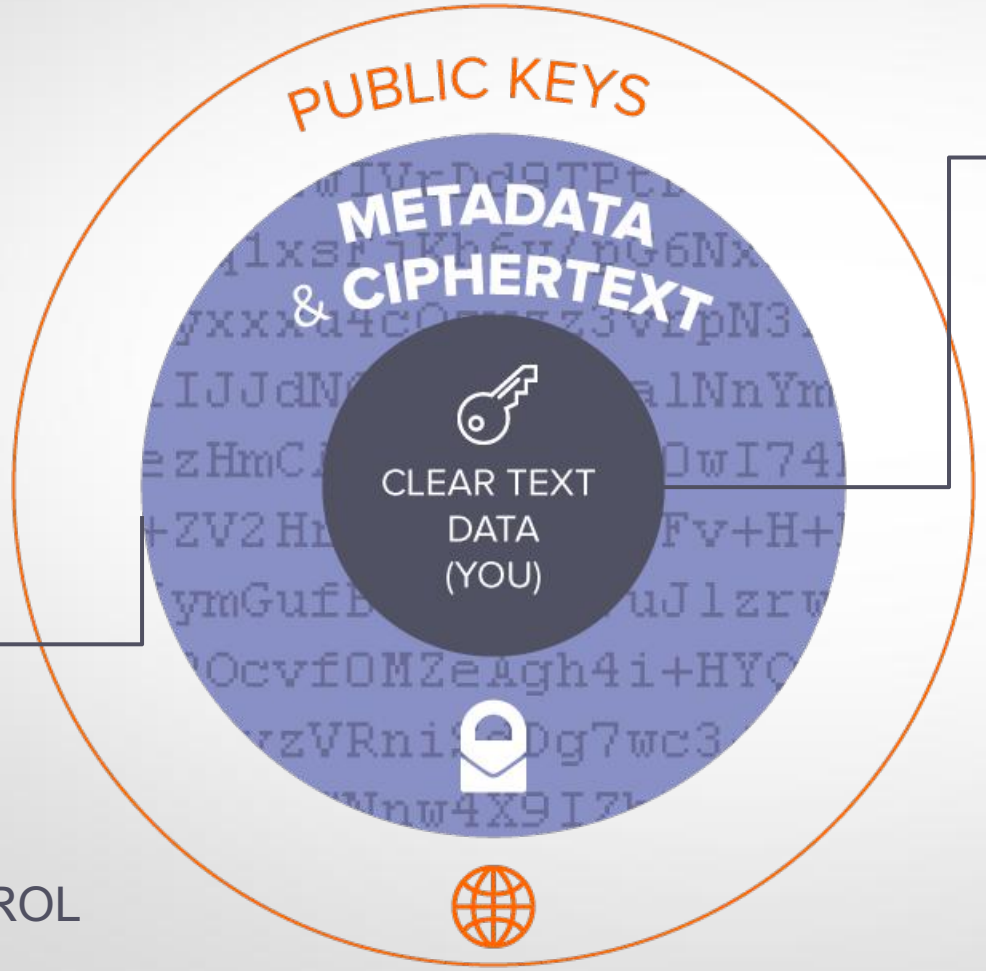
ProtonMail

OPENPGP

- **RFC** 4880
- **Symmetric** encryption of data (fast)
- Public key (**asymmetric**) encryption of symmetric key (slow)
- Allows efficient **server-side manipulation of large, immutable data** (attachments)

ProtonMail

LAYERED ACCESS CONTROL



CLIENT-SIDE
ACCESS CONTROL
(key decryption)

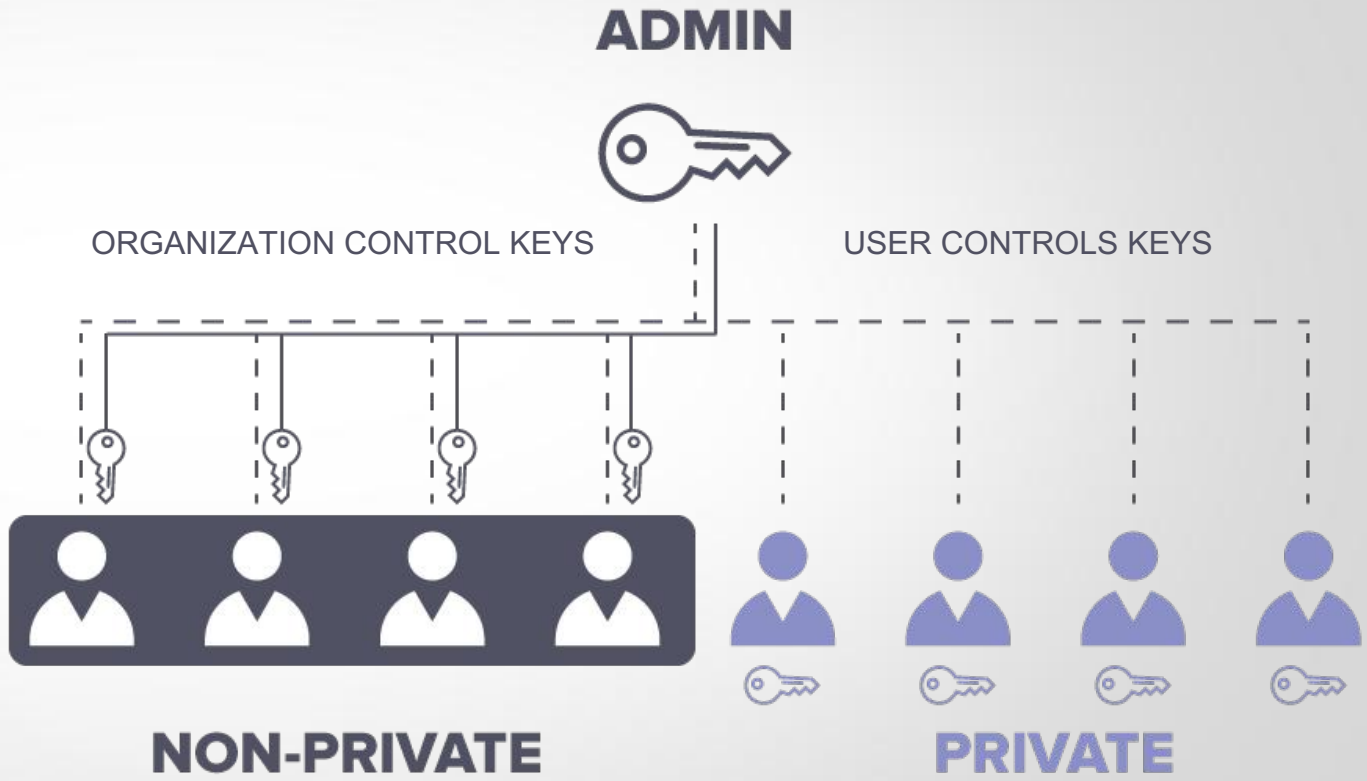
SERVER-SIDE
ACCESS CONTROL
(SRP)

ProtonMail

PROTONMAIL FOR ORGANIZATIONS

ProtonMail

- **New** in 2017
- Individual ProtonMail, user controls keys
- Organizations choose control per-user



SPAM/PHISHING/ABUSE

THE PROBLEM

- Build anything, and some people will want to abuse it
- Deliverability = reputation
- Content is encrypted
- User privacy protection adds complexity

OUR SOLUTION

- Rate monitoring and bans, automated and manual
- Human verification
- Ephemeral analysis of metadata and cleartext (at system edges) as per industry standard
- Behavior patterns

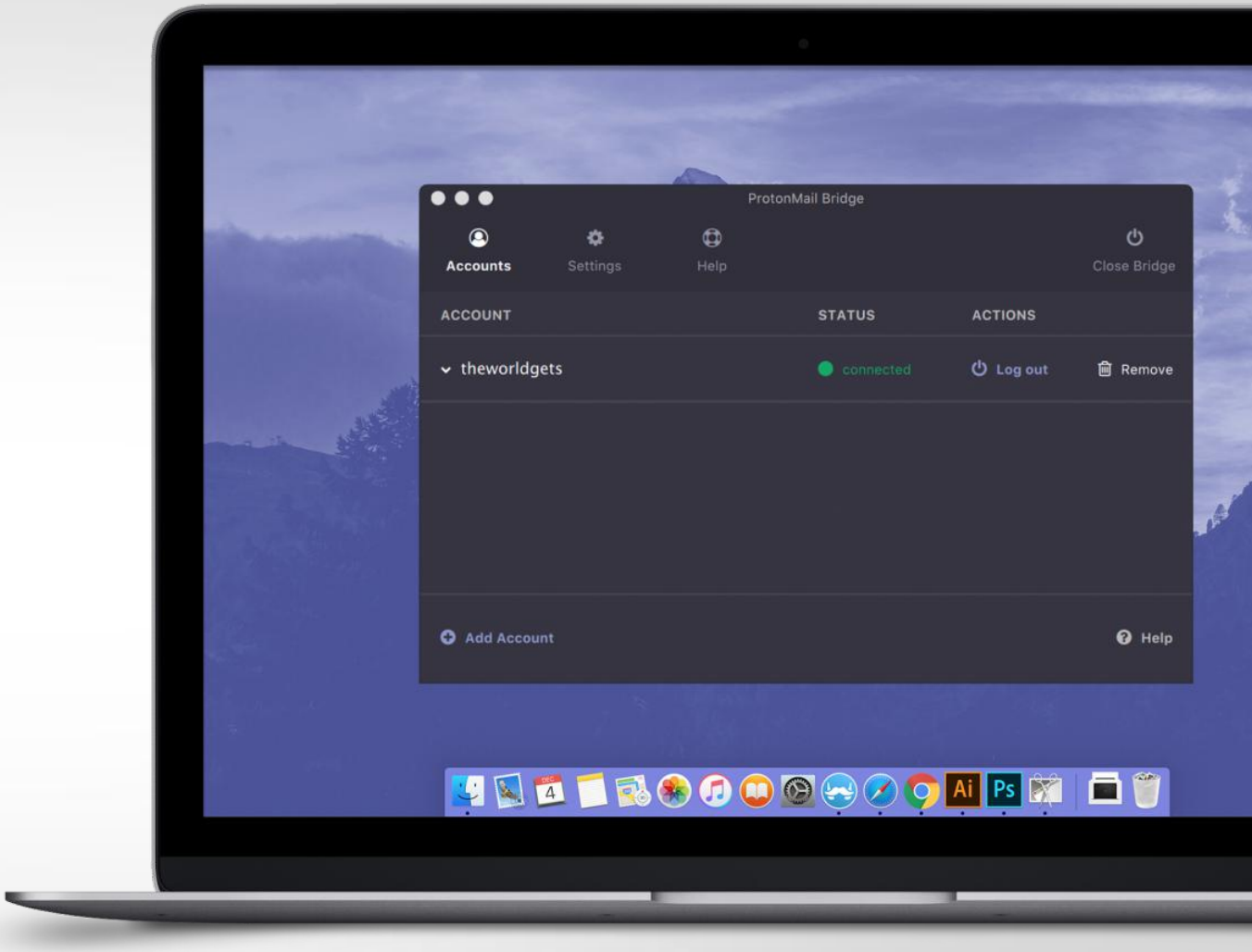
FULL-TEXT SEARCH?

THE PROBLEM

- Content encrypted
- Users expect fast search in a post-Gmail world

OUR SOLUTION

- Custom folders and labels
- Metadata search
- Custom filters
- Local indexing via **ProtonMail Bridge**



ProtonMail

METADATA IS SENSITIVE TOO

THE PROBLEM

- Cleartext metadata sensitive
  - Who and when
  - Subject lines
- E2E encryption not feasible
- Subpoenable

OUR SOLUTION

- Self-hosted infrastructure [**CH only**]
- **Full disk** encryption
- Highly **limited access**

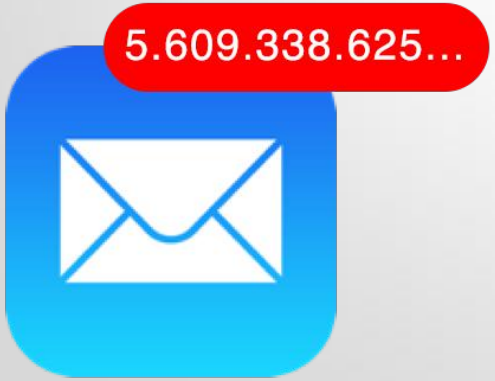
ProtonMail

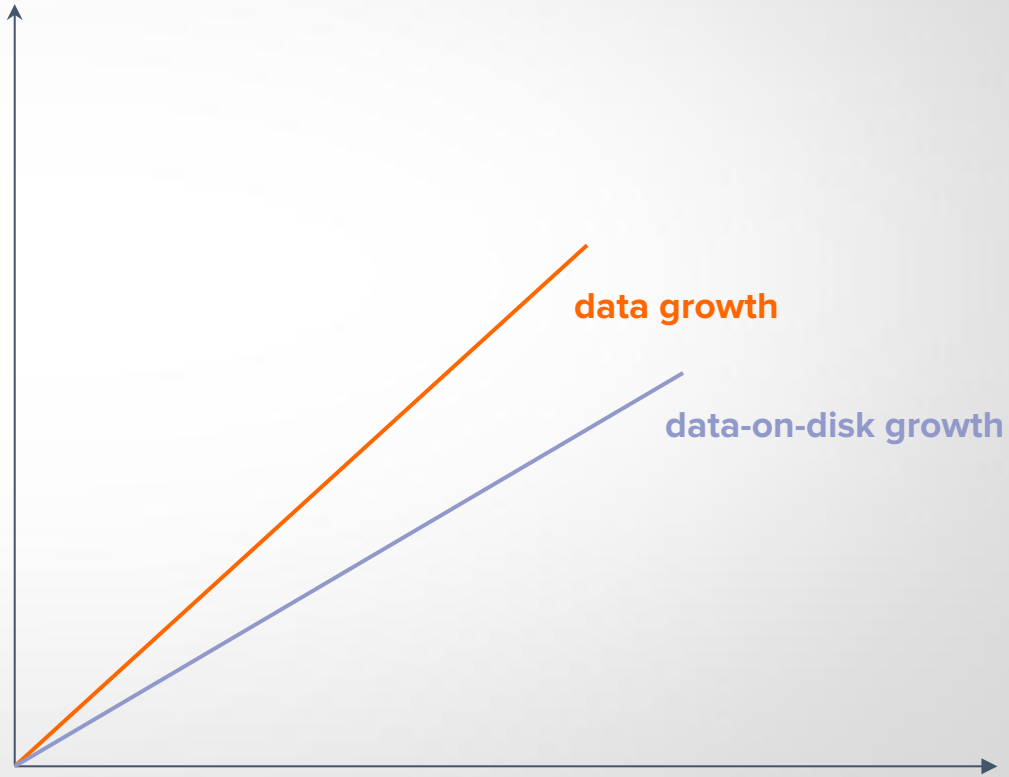
HOW BIG IS YOUR MAILBOX?

ProtonMail

THE PROBLEM

- Rapid data growth
- Incompressible (ciphertext)
- Most of it unique





R&R: REDUNDANCY AND RELIABILITY

THE PROBLEM

- 100% uptime
- All maintenance online
- Self-hosted infrastructure

OUR SOLUTION

- **Multiple** redundant data-centers
- Data replicated within and between data-centers
- Always **at least 3 live copies and several cold backups**
- Automatic/semi-automatic failover, **tested regularly**

ProtonMail

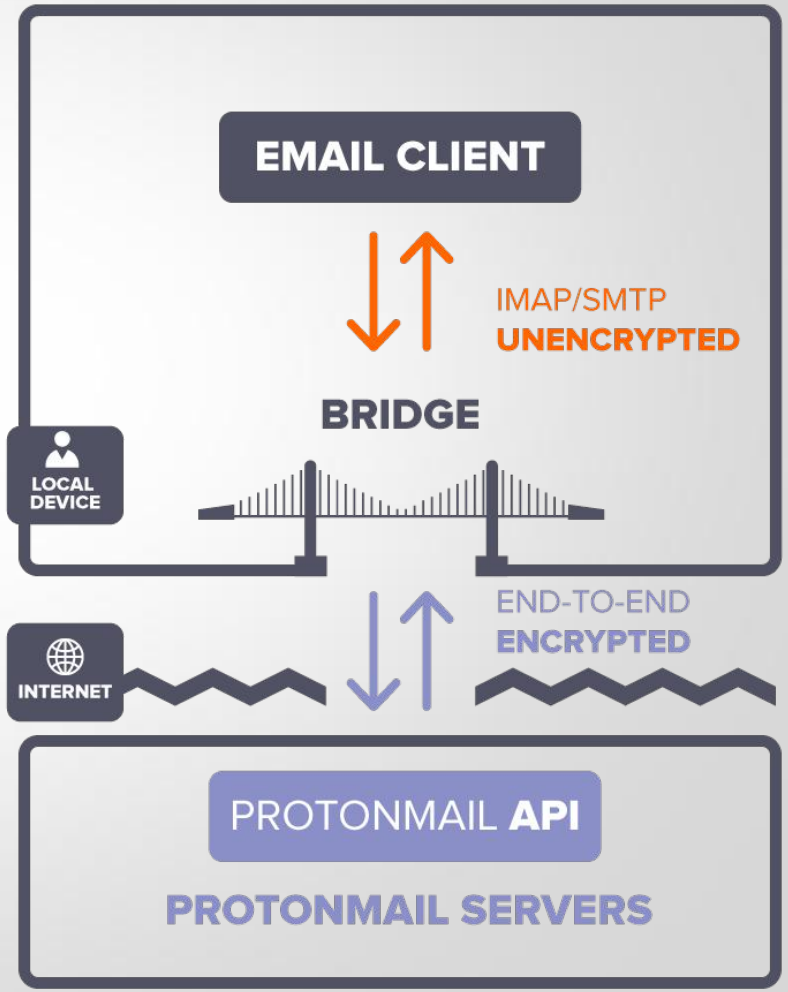
WHEN THE BEST UI IS NO UI

THE PROBLEM

- Menagerie of email clients
- IMAP/SMTP were **not developed with E2E in mind**
- Huge ‘activation energy’ to change email clients

OUR SOLUTION

- ProtonMail **Bridge** daemon runs locally, handling encryption/keys
- All email leaving/entering system is E2E **encrypted**



ProtonMail

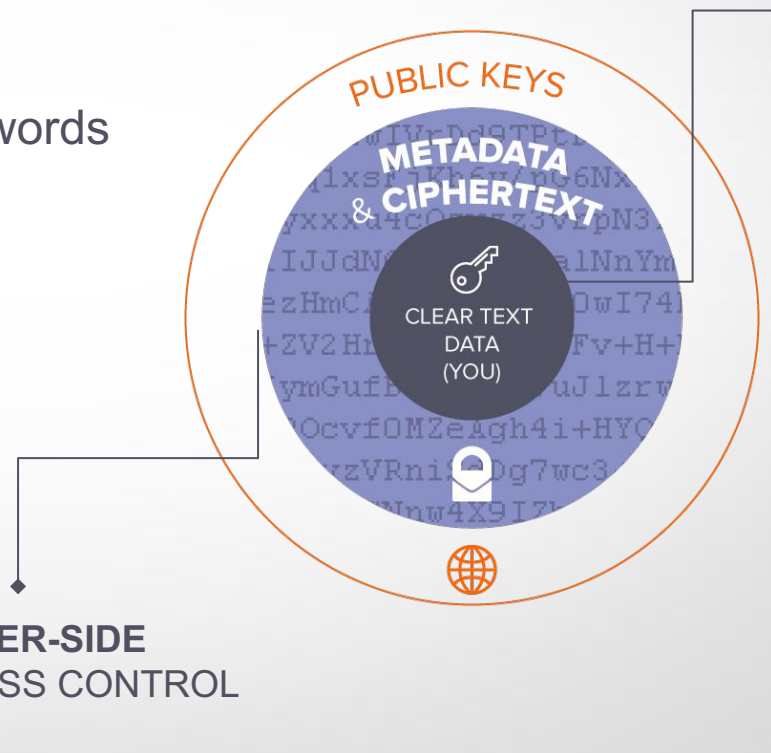
A TALE OF TWO PASSWORDS

ProtonMail

THE PROBLEM

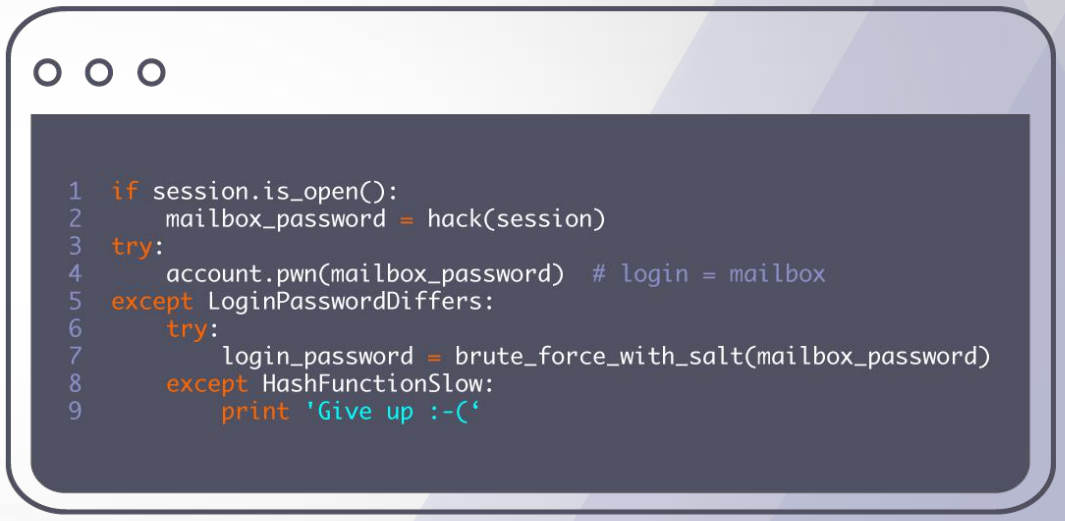
- Original password scheme required two passwords

PROS	CONS
Simple to code **Easy** to understand	**Barrier** to use **Easy** to forget



WHY NOT USE LOGIN PASSWORD FOR MAIL?

- Mailbox password **persists** on clients
  - **Decrypt / encrypt new keys, page refreshes**
- If mailbox = login, open session = account control
- Use slow **hash** function



```
if session.is_open():
    mailbox_password = hack(session)
try:
    account.pwn(mailbox_password)  # login = mailbox
except LoginPasswordDiffers:
    try:
        login_password = brute_force_with_salt(mailbox_password)
    except HashFunctionSlow:
        print 'Give up :-('
```

SECURITY IS AN ONION

DDOS

- BGP routing instead of DNS
- Provider only sees encrypted traffic
- Multiple attacks/week

BRUTE-FORCE API ATTACKS

- Random short cooldowns
- Status code 429 is your friend
- Rate limits based on various criteria

TIMING ATTACKS

- Hash all your tokens

  If database is dumped,

  tokens cannot be used directly

- Use constant-time comparisons
- Selector/verifier pattern

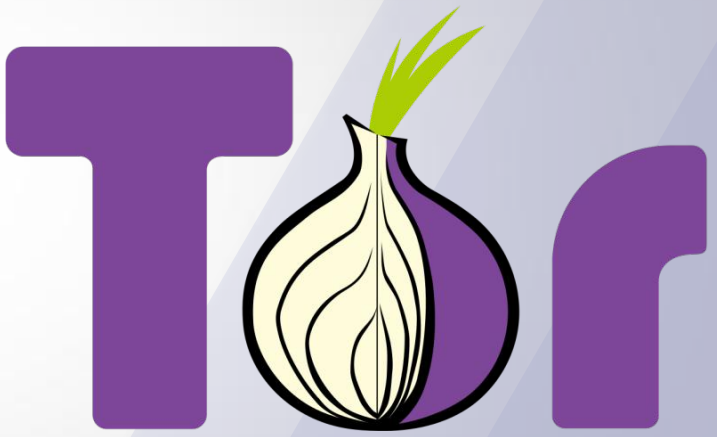
  Selector token for lookup

  Verifier token for comparison

ON THE TOPIC OF ONIONS…

https://protonirockerxow.onion

- Connect to ProtonMail **w/o leaving the Tor network**
- TLS because **users expect it**
- Reasonable domain to **prevent phishing**
- **Not difficult to set up** for medium traffic
- **TLS certificate** and anti-abuse strategies



TRUST ISSUES: **WEBMAIL**

- Webmail is **insecure against**:
  - Malicious server
  - Compromised Certificate Authority
- This is **not a reason not to offer webmail**
  - Required to compete in the industry, full stop
  - Can be secure against other threat models, like passive MITM (very common)
- Using a single page application (SPA) helps avoid refreshes on untrusted networks
- If concerned, use **native apps**, or **local web client from source**

TRUST ISSUES: **KEYS**

- End-to-end **encryption** vs end-to-end **authentication**
- Authenticating key exchange is **very old**, **very difficult problem**
- Individual solution: **key pinning in contacts**
  - Either full key or fingerprint, self-signed
  - If mismatch with key from server, warn user
- Systemic solution: **read-only public registry**
  - CONIKS
  - Google's Key Transparency (KT)
  - Hybrid project based on CONIKS/KT and a blockchain begun with EPFL

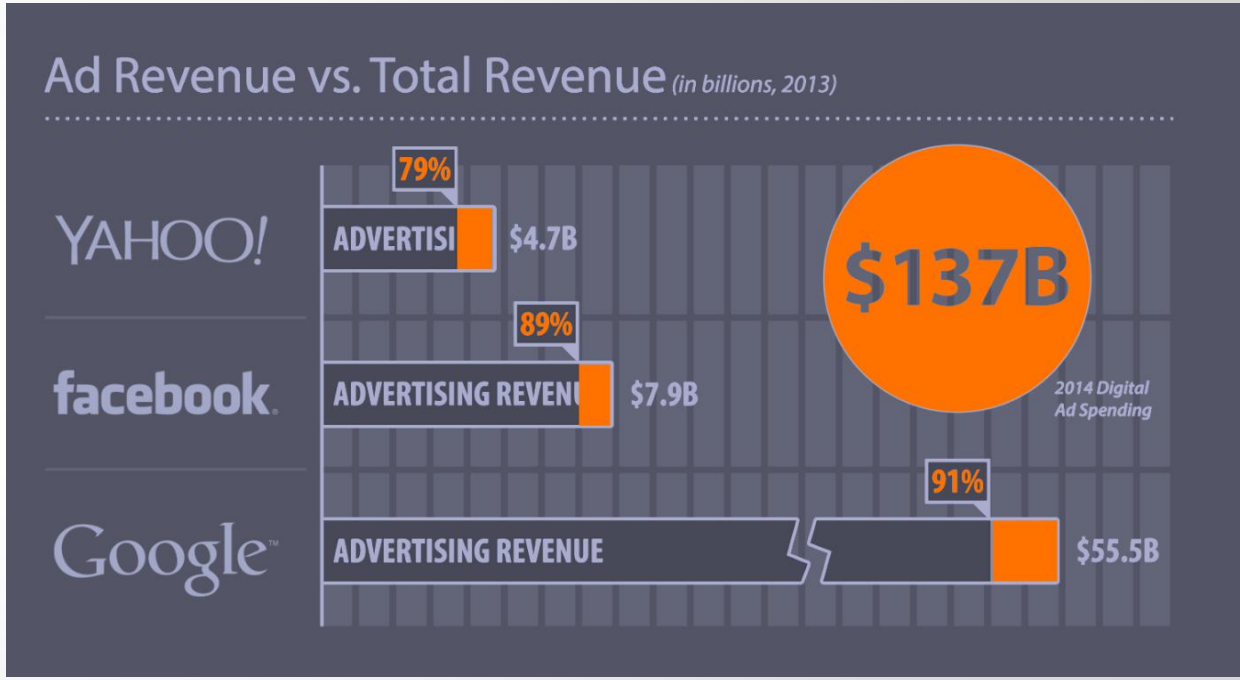
WHEN NOT TO ENCRYPT

- In a **perfect system**, all metadata would be **E2E encrypted**
- Remember that this means **YOU (the developer) lose access to it forever**
- For ProtonMail, this would have **prevented or complicated**:
  - Conversations
  - Filters
  - Metadata search
  - Future features: auto-responder, smart inbox (Social/Promotions/etc)
- **If you cannot compete on features, no one will use your service**

BUSINESS MODEL

ProtonMail

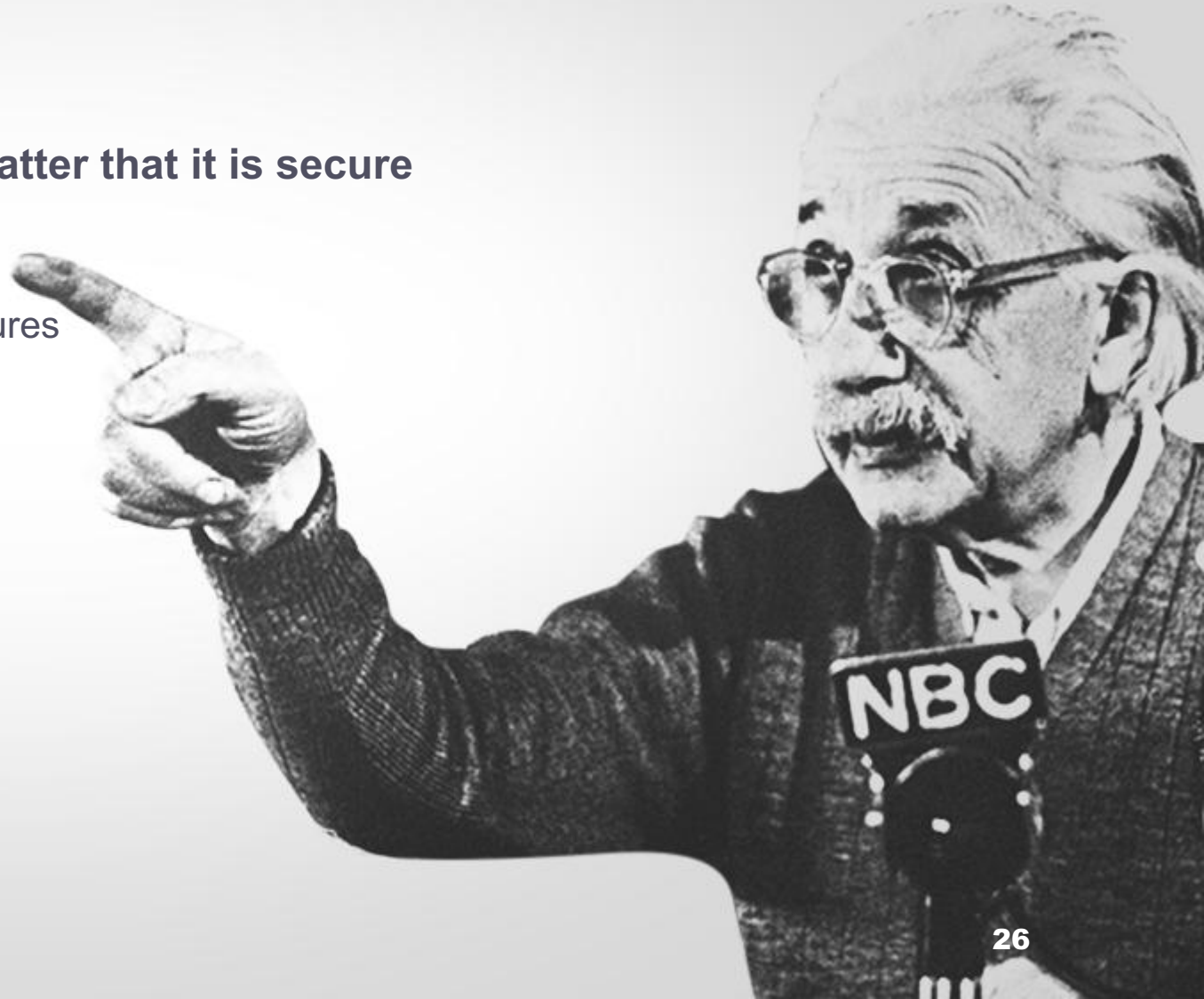
- **If you do not pay for the product, you are the product**
  - Advertisers are Google's customers
  - **They sell you**
- **We do not sell user data**
  - Our business model creates alignment with the user
  - It gives us a financial incentive to protect user data, contrary to other companies trading user data for their own financial gain.
- **We sell**
  - Space & features (more users, labels, folders)
- **Free accounts are part of our mission**



FINAL THOUGHTS

- **If no one uses your service, it does not matter that it is secure**
  - Design and UX are important
  - Do not over-encrypt such that you

  prevent yourself from being competitive on features
- **Refuse to make the perfect the enemy of the good**
- **Email will be around for a long time still, we can and should make it more secure**



ProtonMail

THANK YOU

andy@protonmail.ch

WISH TO SUPPORT A FREE & SECURE INTERNET?
SPREAD THE WORD

@ProtonMail





ProtonMail