Whom Do You Trust?

Privacy and Collaboration in CryptPad
Collaborative Editing
The Privacy We Want

No *untrusted entity* can infer personal information, document content, or collaborators

Image: Sigmund (Unsplash)
Why not Google + co?

India Targets Climate Activists With the Help of Big Tech

Tech giants like Google and Facebook appear to be aiding and abetting a vicious government campaign against Indian climate activists.

Naomi Klein
February 27 2021, 9:00 a.m.
We Need to Control the Software!
It's FOSS, we are safe

The possibility to [...] run your own instance [...] completely removes the need [...] to trust a third party provider and therefore eliminates the need for e2ee.

Jitsi Meet, December 2022
... well, really?

- Can *everybody* run their own instance?
- Really trust system administrator to see *all* your documents?
- Documents are *not* ephemeral!
End-to-End-Encryption (E2EE)
It's E2EE, we are safe

With Google Workspace Client-side encryption (CSE), content encryption is handled in the client's browser before any data is transmitted.

Google
... well, really?

- Metadata
- A cryptosystem should be secure, even if everything about the system, except the key, is public knowledge.

Kirchoffs Principle
What is CryptPad?
How Does CryptPad Encrypt?

32e19a708
asd989e2f
c08394d1d

Hello
there

394d1

394d1

394d1

Hello

Hello
Trust: Server ≠ Active Attacker

- Practical: Distribute the client code
- Theoretical: Server can always delete files
Honest-but-curious Attacker

Server doesn't act maliciously, but watches you

Image: eff.org
G7 leak: Pirate Party server seized by police

For the publication of secret documents, they used, among other things, the CryptPad instance of the Pirate Party, which allows the public and free sharing of documents. Server hoster Hetzner was informed about the ongoing investigations and subsequently took the servers off the network, the party writes further.
Protect The Server From Its Users
We Need Open Source *and* E2EE for Good Trust Assumptions
David Benqué - CryptPad Team Lead
Aaron MacSween - Privacy Engineer
Yann Flory - Privacy Engineer
Mathilde Grünig - Community & Support
Theo von Arx - Cryptography Researcher
Arnaud Laprévote - Research and Business Lead
Ludovic Dubost - XWiki CEO