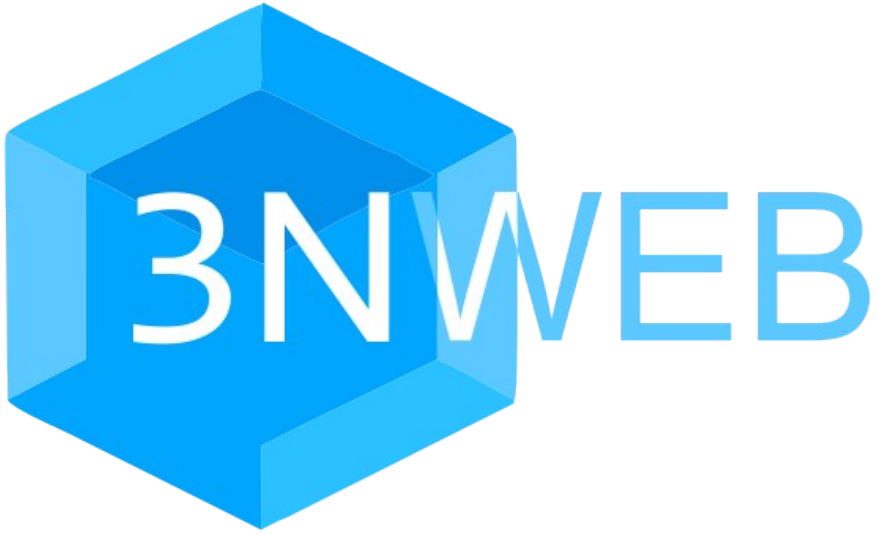


Architectures

User Freedoms

Yale Reading Group
October 2022

1.1. Tussle in the Cyberspace

2. PRINCIPLES

The thesis of this paper is that the future of the Internet will increasingly be defined by tussles that arise among the various parties with divergent interests, and that the technical architecture of the Internet must respond to this observation. If this is so, are there principles to guide designers, and mechanisms that we should use in recognition of this fact?

"Tussle in Cyberspace: Defining Tomorrow's Internet", DOI 10.1145/633025.633059, August 2002,
https://groups.csail.mit.edu/ana/Publications/PubPDFs/Tussle2002.pdf

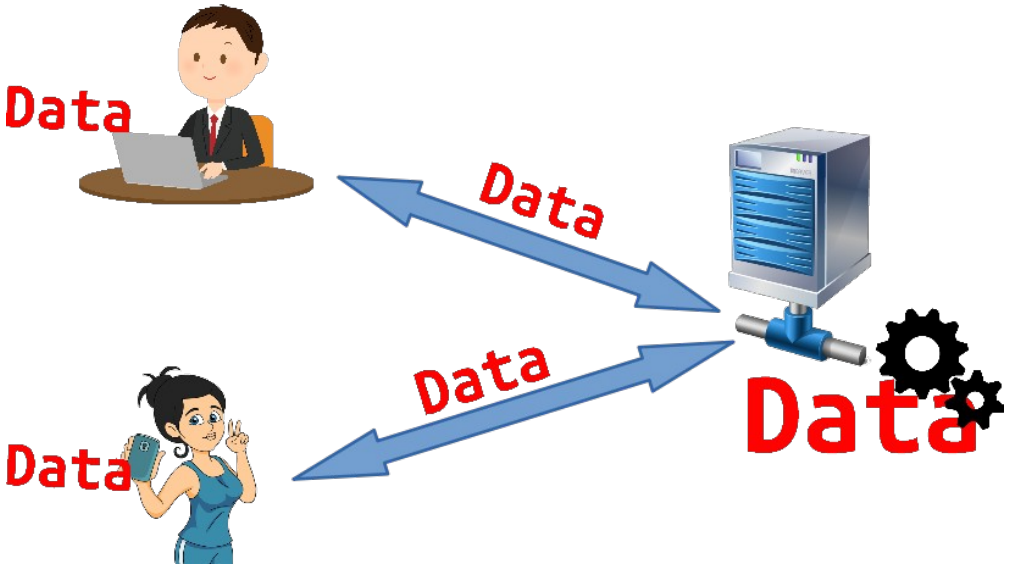
1.2. 18 years later, RFC 8890, The Internet is for End Users

Many who participate in the IETF are most comfortable making what we believe to be purely technical decisions; our process favors technical merit through our well-known mantra of "rough consensus and running code."

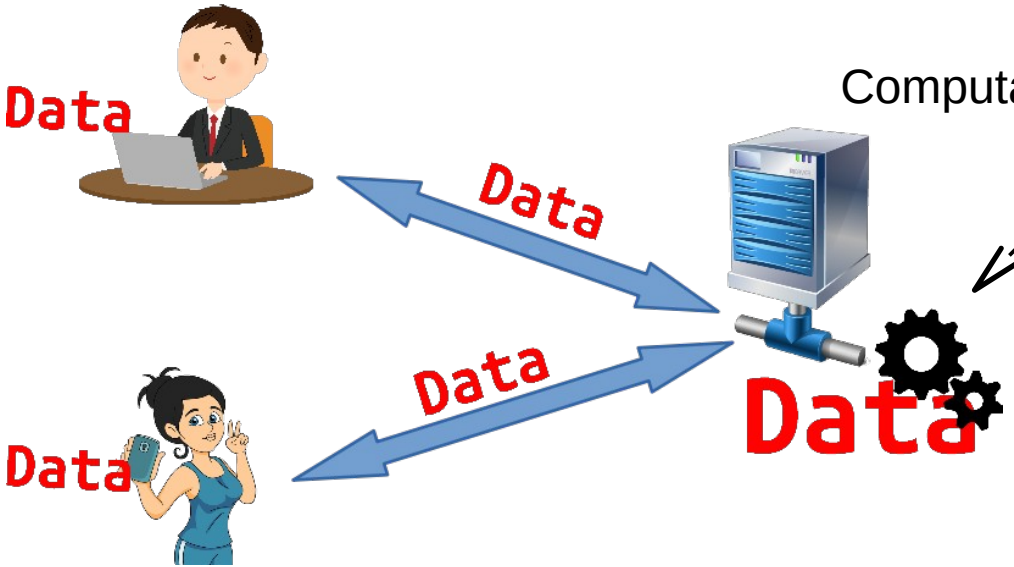
Nevertheless, the running code that results from our process (when things work well) inevitably has an impact beyond technical considerations, because the underlying decisions afford some uses while discouraging others. While we believe we are making only technical decisions, in reality, we are defining (in some degree) what is possible on the Internet itself.

This impact has become significant. As the Internet increasingly mediates essential functions in societies, it has unavoidably become profoundly political; it has helped people overthrow governments, revolutionize social orders, swing elections, control populations, collect data about individuals, and reveal secrets. It has created wealth for some individuals and companies while destroying that of others.

2.1. Simple Architecture, dating well back



2.1. Architecture helps Digital Feudalism

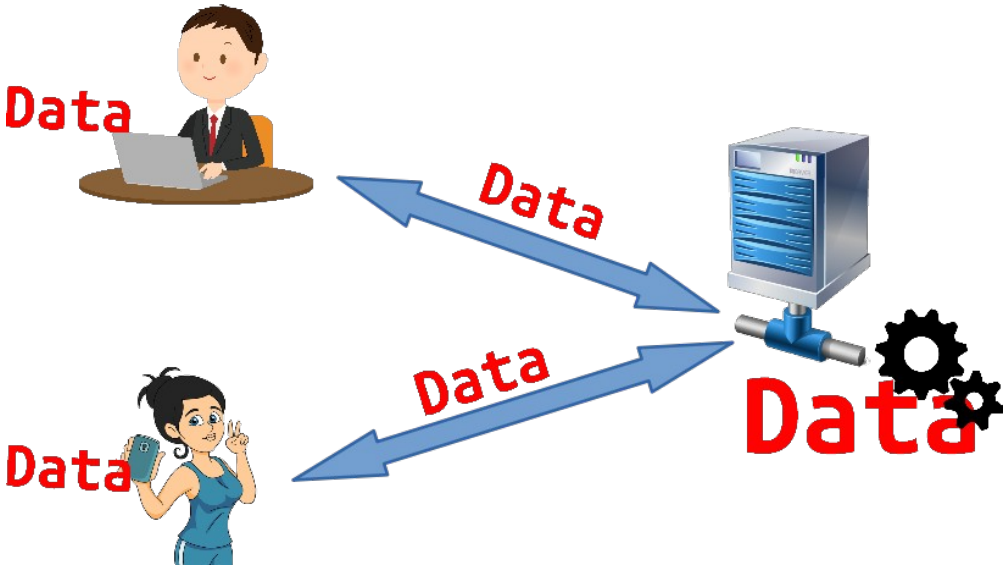


Computation on server gives someone else total, abusive feudal control over end users' digital lives.

It's a feudal world out there. ...
Traditional computer security centered around users. ... This model is breaking, largely due to two developments:
1. New Internet-enabled devices where the vendor maintains more control over the hardware and software than we do — like the iPhone and Kindle; and
2. Services where the host maintains our data for us — like Flickr and Hotmail.

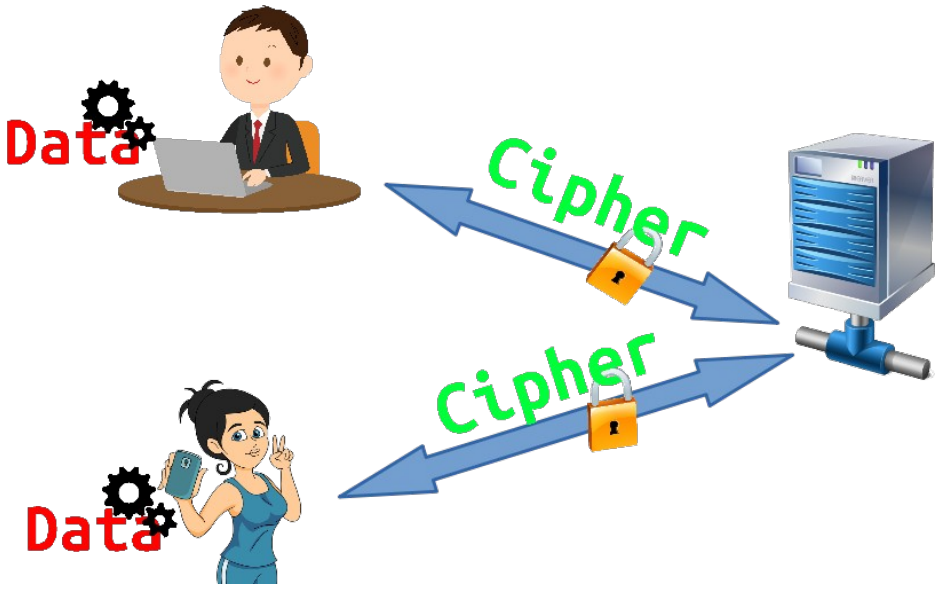
Bruce Schneier, December 2012 in https://www.schneier.com/blog/archives/2012/12/feudal_sec.html

2.1. Architecture helps Digital Feudalism

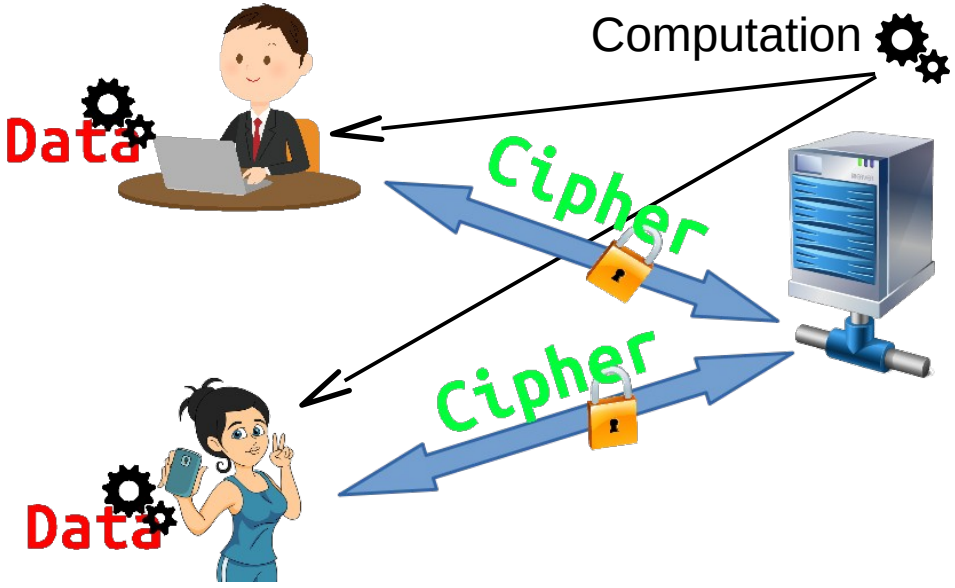


Bruce Schneier, December 2012 in https://www.schneier.com/blog/archives/2012/12/feudal_sec.html

2.2. Architecture with E2E encryption

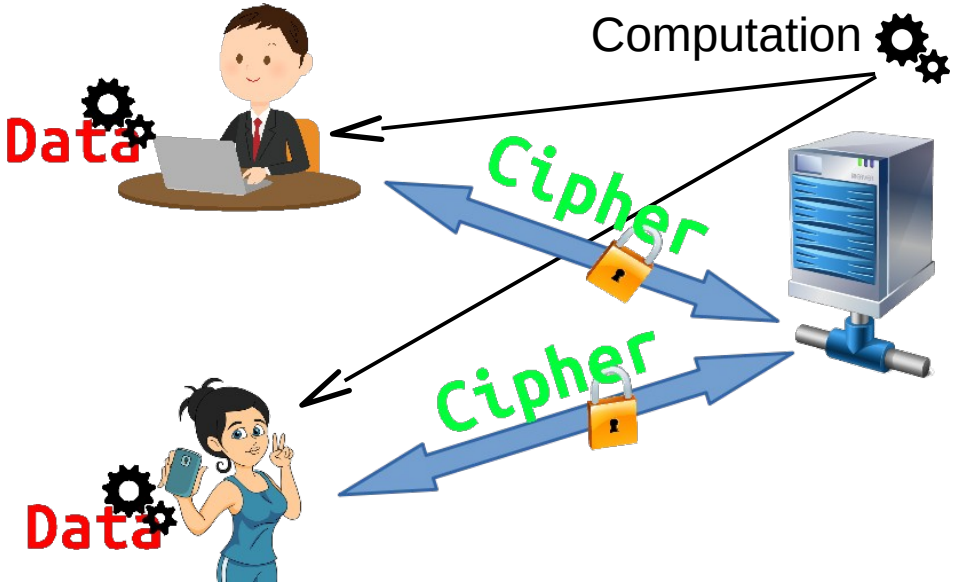


2.2. Architecture promotes data ownership



Computation ⚙ on client sides returns data ownership to users

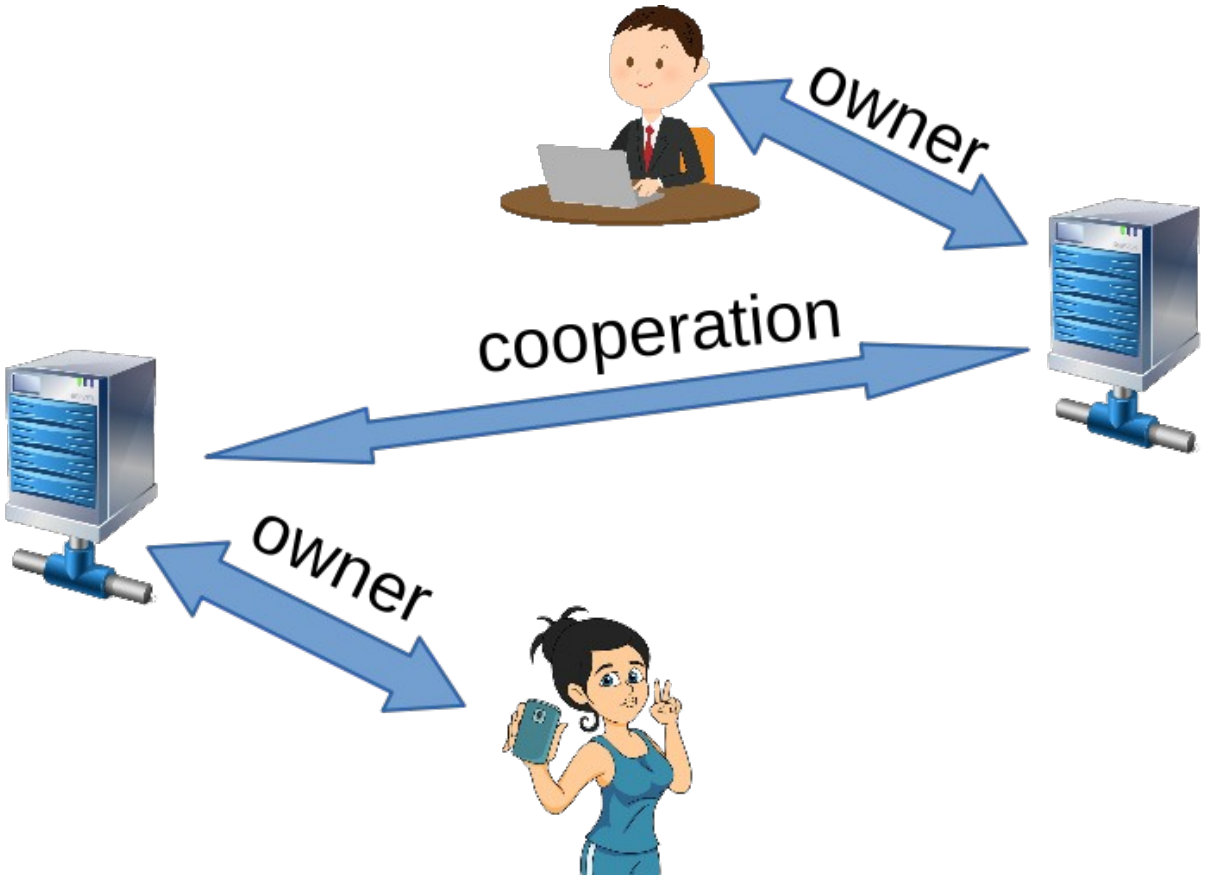
2.2. Architecture promotes data ownership



Computation ⚙ on client sides returns data ownership to users

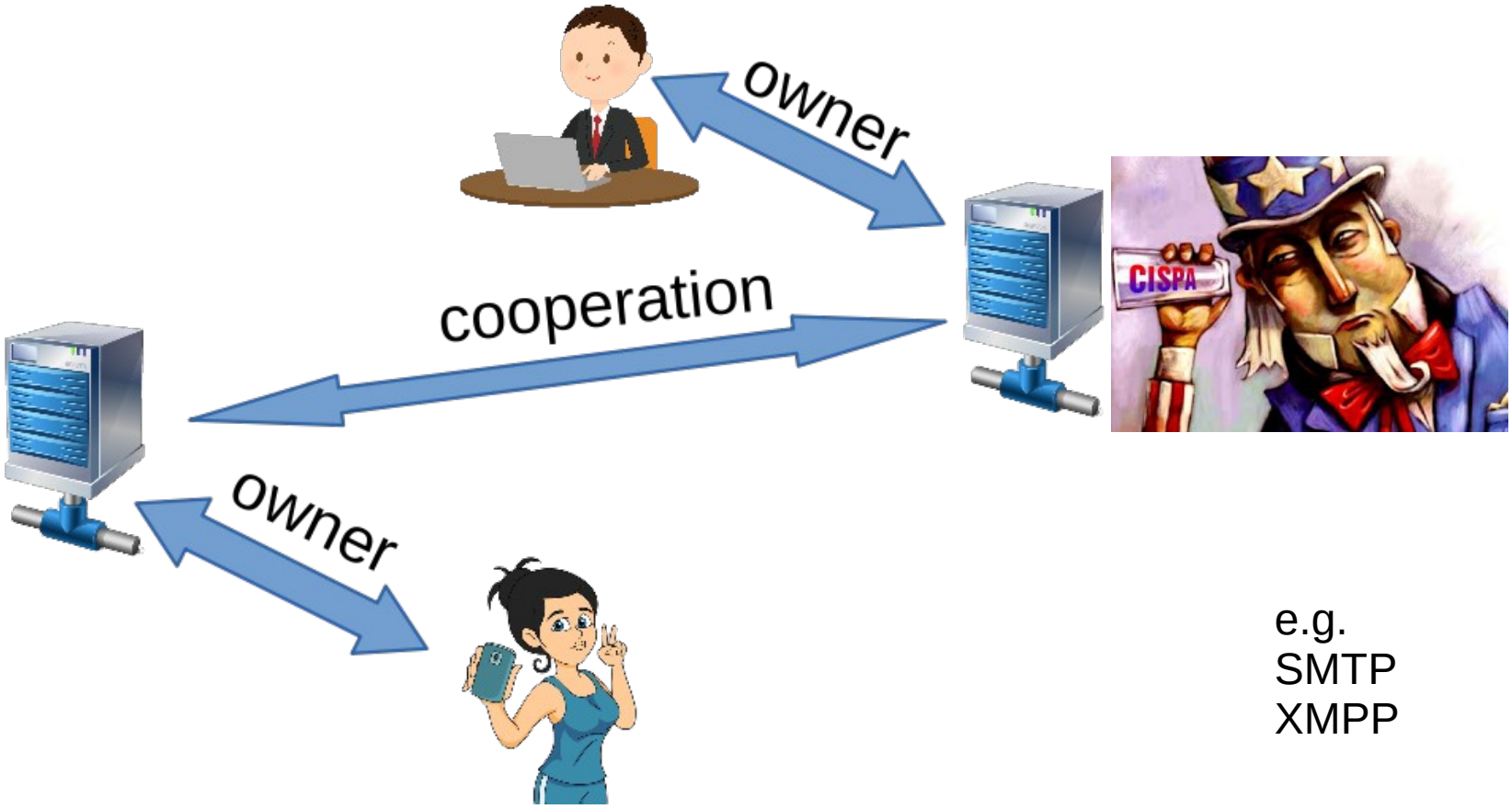
Server still looks
too **centralized**,
too **monopolistic**

2.3. Classical Federation



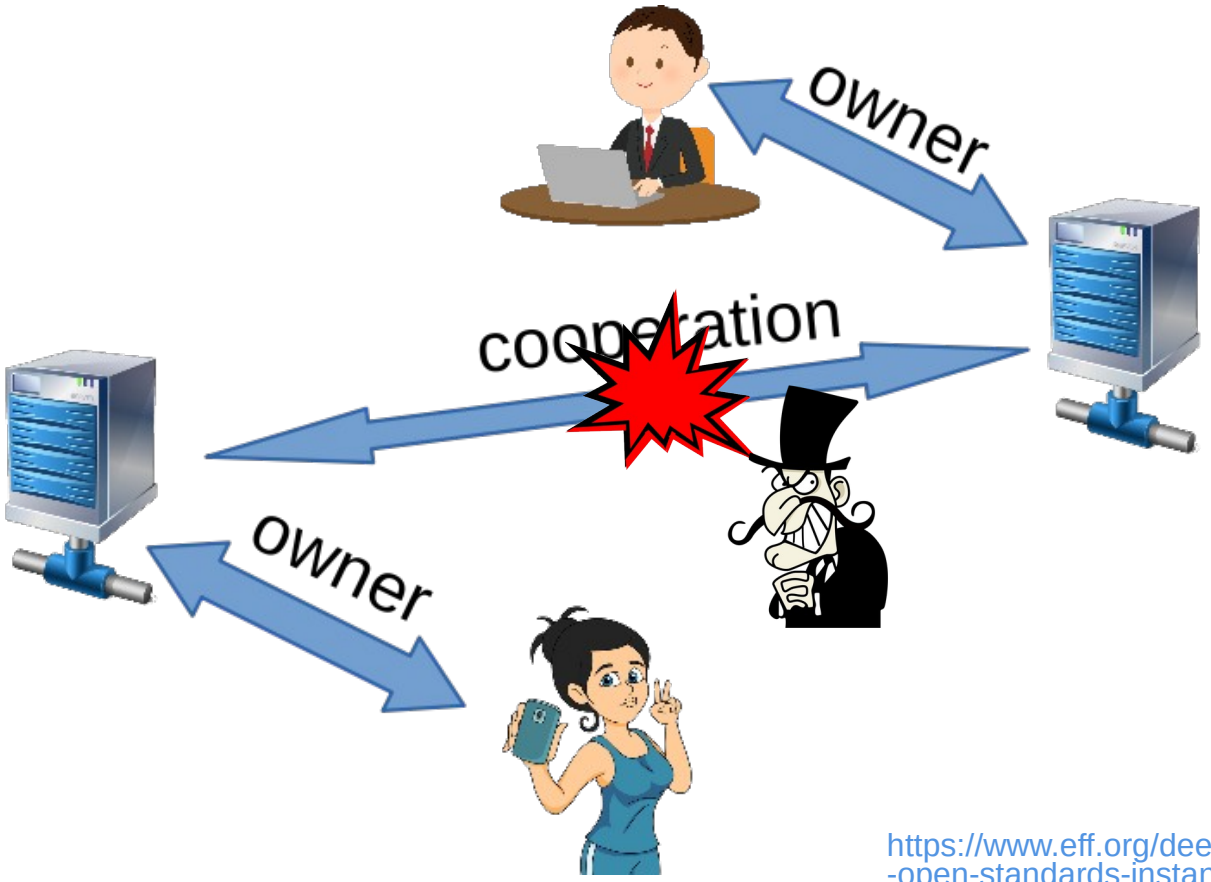
e.g.
SMTP
XMPP

2.3. Classical Federation & metadata



e.g.
SMTP
XMPP

2.3. Classical Federation in a tussle



e.g.
SMTP
XMPP

https://www.eff.org/deeplinks/2013/05/google-abandons-open-standards-instant-messaging

2.3. Arguments with the false choice?

Signal

Reflections: The ecosystem is moving

moxie0 on 10 May 2016

At Open Whisper Systems, we've been developing open source "consumer-facing" software for the

Stuck in time

In some circles, this has not been a popular opinion. When someone recently asked me about federating an unrelated communication platform into the Signal network, I told them that I thought we'd be unlikely to ever federate with clients and servers we don't control. Their retort was "that's dumb, how far would the internet have gotten without interoperable protocols defined by 3rd parties?"

matrix

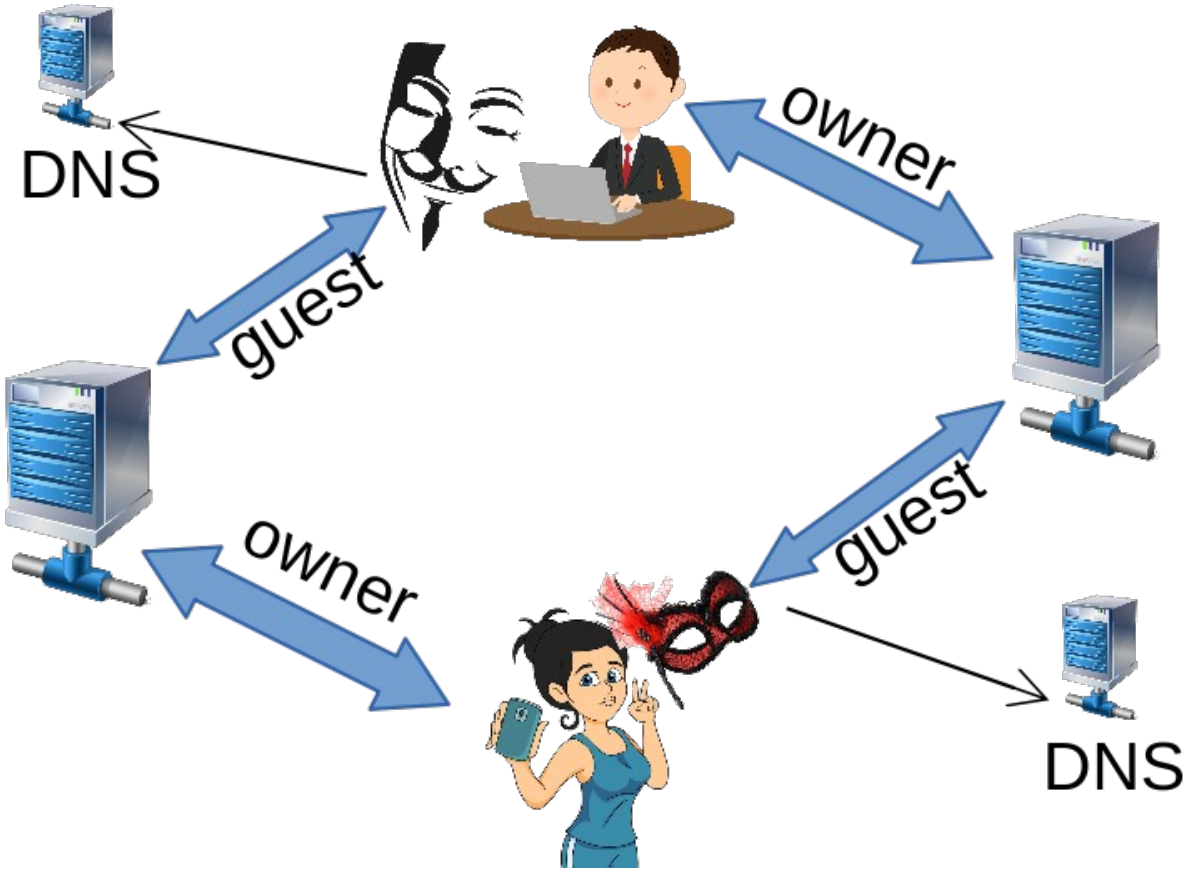
On Privacy versus Freedom

2020-01-02 — Thoughts — Matthew Hodgson

A few years ago, back when Matrix was originally implementing end-to-end encryption, we asked Moxie (the project lead for Signal) whether he'd ever consider connecting Signal (then TextSecure) to Matrix. After all, one of Matrix's goals is to be an interoperability layer between other communication silos, and one of the reasons for us using Signal's Double Ratchet Algorithm for Matrix's encryption was to increase our chances of one day connecting with other apps using the same algorithm (Signal, WhatsApp, Google Allo, Skype, etc). Moxie politely declined, and then a few months later wrote "The ecosystem is moving" to elaborate his thoughts on why he feels he "no longer believes that it is possible to build a competitive federated messenger at all."

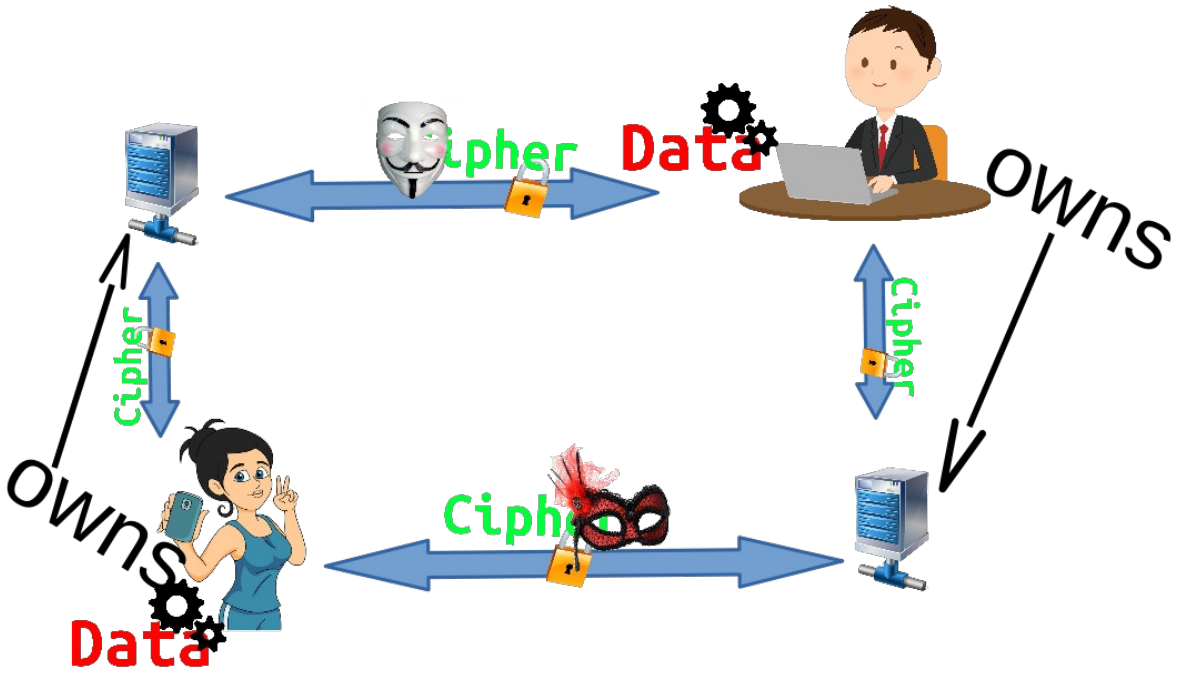
2.3. Web-style Federation

(federated experience without server-to-server cooperation)



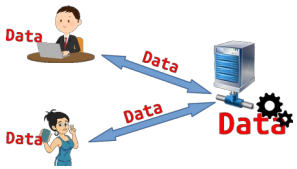
e.g.
Wordpress,
NextCloud

2.4. We must combine best for End Users

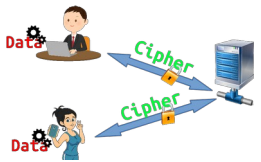


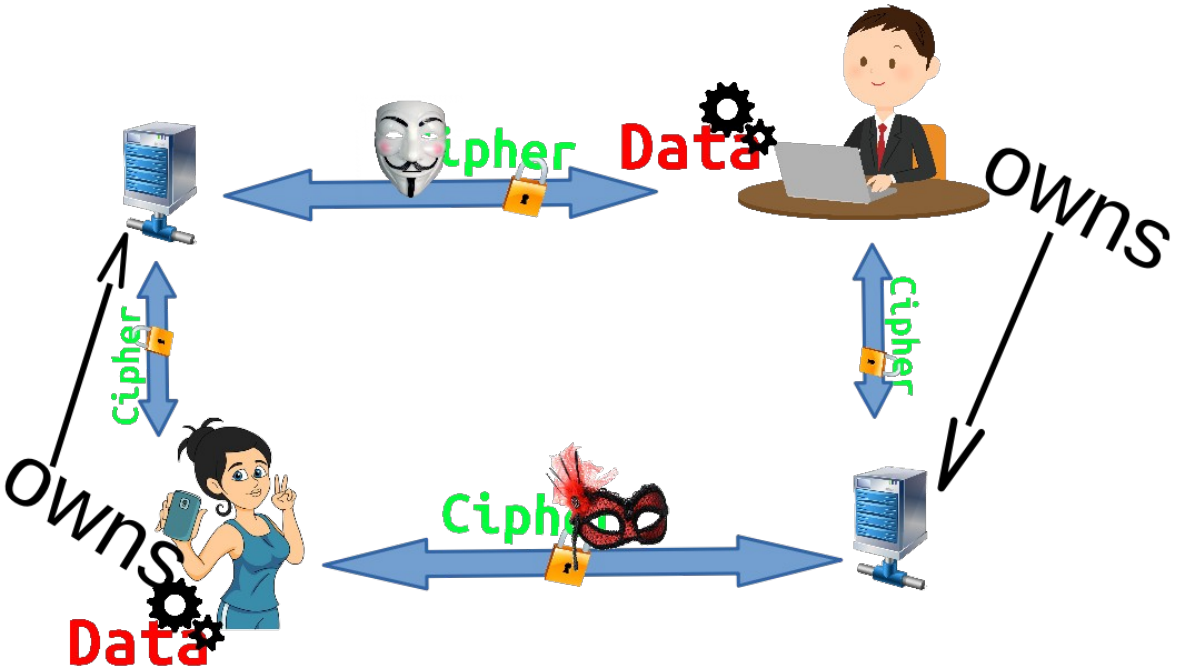
2.4. Digital Freedom

Digital Feudalism



Data Ownership



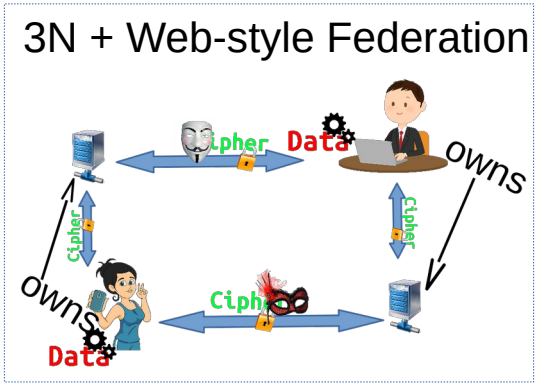


3.1. 3N principle for tussle-safe client-server communication

- No plain text user content should be given to server.
- No unnecessary metadata should be present or generated in client-server interaction.
- Nothing can be abused on the server, when the first two criteria are met.

3.2. 3NWeb protocols

(Application Layer 7 in OSI model)



3NWeb is a set of utility services forming base for apps

App needs	Functionality	Protocol
Disk	Persisting data	3NStorage
Pipe	Messaging	ASMail
User creds	Identification	MailerId

3.3. Overall stack

Apps: what users use, what ultimately has value for end users

API and formats' on 3NWeb App and OS boundary

"OS": environment layer for apps on user device(s)

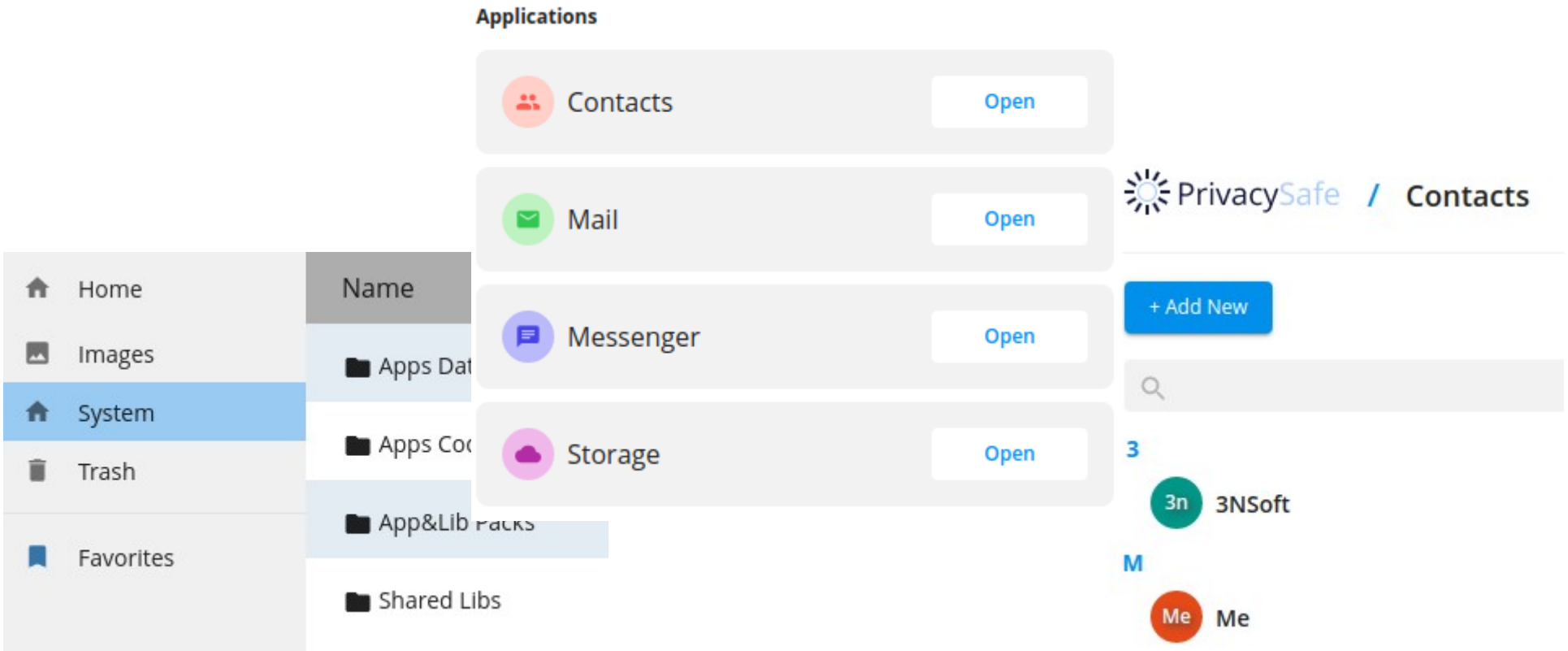
3NWeb protocols

Utility Services: 3NStorage, ASMail, MailerId

3.4. APIs, formats & protocols (at IEEE)

Standards	Type	Needed by	Details
Public Key Login (PKL)	protocol	MailerId, ASMail, 3NStorage	Credentials based access without 3rd parties (e.g. identity providers).
MailerId	protocol	ASMail, 3NStorage	Non-tracking identity, based on Mozilla's BrowserId approach, minus hacked browser part.
ASMail	protocol	OS' messaging functionality	3N-observing Web-style federated messaging protocol
3NStorage	protocol	OS' data persistence	3N-observing Web-style federated bulk storage protocol
XSP file format	format	ASMail, 3NStorage	AEAD (Authenticated-Encryption with Associated Data) format to pack NaCl ciphers (XSalsa+Poly)
File content packing	format	OS' file system functionality	While XSP packs encrypted segments it is beneficial to also have an additional file content segments' packing for efficiency in always encrypting, atomic versioning, and reduction of metadata in synchronization via servers.
OS to Apps IPC	api	Apps	Base approach to IPC between 3NWeb Apps and OS layers
File system objects	api	Apps	File system objects (capabilities) given to Apps
ASMail messaging	api	Apps	ASMail messaging object (capability) given to Apps
Apps and services IPC	api	Apps, OS	Meshing functionality as an application of UNIX philosophy
App manifest	format	OS	App manifest asks for capabilities, else OS doesn't give them

Demo


Applications
Contacts
Open
Mail
Open
Messenger
Open
Storage
Open
PrivacySafe / Contacts
+ Add New
3
3n
3NSoft
M
Me
Me
Home
Images
System
Trash
Favorites
Name
Apps Dat
Apps Coc
App&Lib Packs
Shared Libs