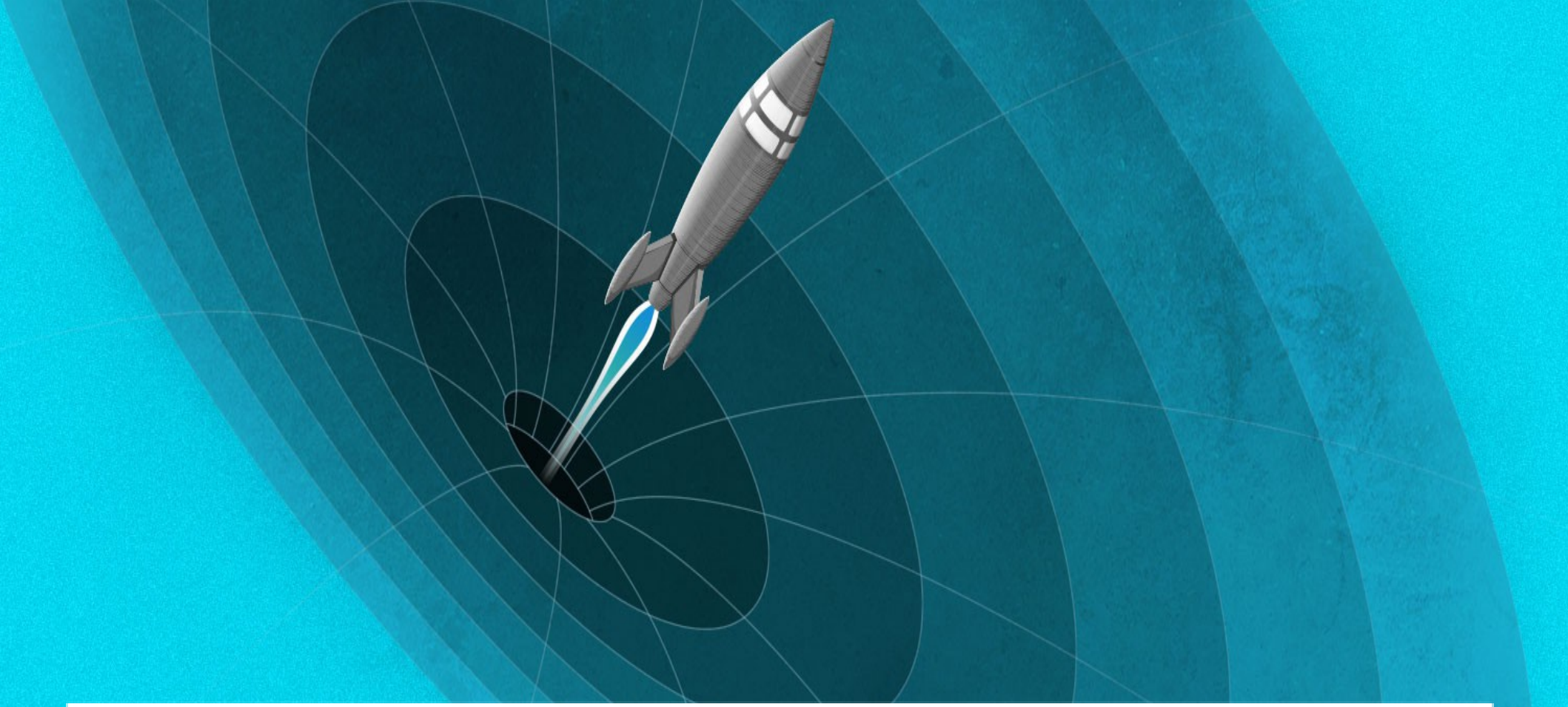
PAST WORK

NO MORE MITM ON THE WEB!

USE CERTIFICATE PATROL ADD-ON FOR FIREFOX


YOU
BROKE
THE INTERNET



WE'LL MAKE OURSELVES A GNU ONE

Theory and practice of a completely encrypted and obfuscated new Internet stack, enabling us to unfold a carefree digital living.

YOUBROKETHEINTERNET.ORG

about:

SECRECY OF CORRESPONDENCE + FREEDOM OF ASSEMBLY

for Humankind … … *by default*

Why Metadata Matters

- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.
- They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.

about:

PREDICTABLE ELEGIBLE VOTERS:

DEMOCRACY @ RISK.

MANIPULATION BECOMES CHEAP.

IT'S NOT ABOUT SELF-DETERMINATION

MOST THINGS A PERSON DOES ON THE INTERNET AFFECTS OTHERS...

... AND DEMOCRACY AS A WHOLE.

BEING ALLOWED TO SELL YOUR "PERSONAL" DATA...

IS LIKE BEING ALLOWED TO DRIVE A CAR AT NIGHT WITHOUT LIGHTS ON.

YOU ARE ACTING IRRESPONSIBLE AND PUTTING OTHERS AT RISK.

UPGRADE YOUR THINKING OF THE CONSTITUTION:

THE CONSTITUTION ISN'T

ONLY WHAT IS WRITTEN IN THE LAW.

IT IS ALSO WHAT WAS ORIGINALLY INTENDED BY ITS AUTHORS – TO

SAFE-GUARD DEMOCRACY.

UPGRADE YOUR THINKING OF THE CONSTITUTION:

THEY COULDN'T PREDICT THAT COMMUNICATION METADATA WOULD THREATEN DEMOCRACY, BUT IT IS LEGALLY VIABLE TO INTERPRET "SECRECY OF CORRESPONDENCE" THIS WAY.

LET'S ADMIT IT...

THE WEB IS ILLEGAL

WE NEED TO FIX IT.

SORRY FOLKS, BUT...

THE MARKET CAN'T FIX IT

there is no business model for constitutional fundamentals...

IS IT WORTH TRADING DEMOCRACY IN FOR…

– anti-constitutional **BUSINESS MODELS**
that *(as a side effect)* destroy
the **"MARKET"** by asymmetry…

– **BIG DATA ANALYSIS** to detect
ANIMALPEDOTERRORISM that
(as a side effect) empowers the agencies
to impede democratic new thinking…

(EU) LEGISLATION PROPOSAL:

OBLIGATORY ANONYMIZED AND END-TO-END ENCRYPTED COMMUNICATIONS IN ALL TELEPHONY AND COMPUTING APPLIANCES SOLD AFTER 201X.

= LET'S FIX THE INTERNET BY LAW...

PROBLEMATIC OPERATIONS

– CODE EXECUTION
on user devices

+ sandboxing
+ limited/properly timed permissions*
+ open sourcing outer shell
+ … hardware!

*) see also Bal/Rannenberg

PROBLEMATIC OPERATIONS

– UNSAFETY OF USER DATA
confided to entities on the net

+ move apps to the device
+ detach identity from app data
+ impede long-term aggregation*


CAMERA ACCESS:
– one photo
– video stream
NET ACCESS:
– cryptographic recipient
– authenticated or anonymized
– protocol restrictions
ETC.
CIVIL RIGHTS DEFENDER CHIP
– free hardware
– free software
iOS/ Android-style SANDBOXES

GNU INTERNET ARCHITECTURE? SOMETHING LIKE...

PUBLIC-KEY-BASED ROUTING
DISTRIBUTED HASHTABLE
CRYPTO/ONION RELAY MESH
DATA DISTRIBUTION PLAN
PRIVATE SOCIAL GRAPH

Technische Unive
Department of C
Network Architec

Tel +49
Fax +49-8
christian@grot
http://grothoff.
GPG Fingerp

PhD (UCLA)

RESOLUTION & DISCOVERY

PUBLIC-KEY-BASED ROUTING

– NO MORE BUZZWORD.COM
+ ADVERTIZE BY QR-CODE
+ ADD VIA BLUETOOTH
+ ADOPT BY SOCIAL GRAPH
~ CONFIRM BY SHARED SECRET
(IF NECESSARY BY VOICE)

GNU INTERNET ARCHITECTURE

DISTRIBUTED HASHTABLE

REPLACE DNS
REPLACE X.509
(AKA CERTIFICATION AUTHORITIES)
REPLACE SERVER FEDERATION
NO MORE SERVER ADMINISTRATION

GNU INTERNET ARCHITECTURE

CRYPTO/ONION RELAY MESH

TOR, ANYONE?

I2P, GNUNET, FREENET,
CJDNS, RETROSHARE,
ZYRE, RHYZOME,
BRIAR, NET2O.

GNU INTERNET ARCHITECTURE

MULTICAST
DATA DISTRIBUTION TREES
= SCALABILITY

BITTORRENT FOR EXAMPLE
→ HIGH POPULARITY APPS

... BLOCKCHAIN?

GNU INTERNET ARCHITECTURE

PRIVATE SOCIAL GRAPH

... DISTRIBUTED AMONG PEOPLE
... USEFUL FOR DISCOVERY!

RESEARCH SAYS:

- ANONYMOUS MULTICAST DISTRIBUTION TREES, YES!

- SOCIAL GRAPH PROTECTS AGAINST SYBIL ATTACKS

- SOCIAL ONION ROUTING COULD BE SAFER THAN TOR

GNU INTERNET APPS

MAIL, MESSAGING,
SOCIAL NETWORKING,
TELEPHONY,
CONFERENCING,
... EVEN THE "WEB,"
BUSINESS TRANSACTIONS ETC.

GNU INTERNET APPS

CRYPTOGRAPHIC
ANONYMOUS
MICROPAYMENT

SO YOU NO LONGER PAY
WITH YOUR DATA...

GNU INTERNET APPS

NO MORE LOCATION TRACKING

WE PAY OUR TELECOM RELAYS ANONYMOUSLY...

GNU INTERNET APPS

PUSH WEBSITES
VIA PUBSUB
ONTO MY DEVICE...
LIKE AN APP?

CHANGE THE BUSINESS MODEL

MANY-TO-MANY SCALABILITY

Multicast & PubSub

Faceboogle
Twitter

PSYC

BitTorrent

blackad

NNTP
IRC

CCN

vs Storage
& Replication

ONE-TO-ONE APPLICATION

PGP
OTR

Microsoft

RetroShare

Briar

Pond
TorChat
Globaleaks
Wikileaks

Tri

Tribler's Tor over UDP

I2PBote
etc

ZeroMQ

cjdns

Jitsi

Tox

Skype

Tahoe-LAFS

freenet

CRYPTO ROUTING

Confidentiality
Authentication
Repudiability
Untraceability
Unlinkability

Tor

GNUnet

I2P

X.509
DNS & DANE
SMTP & XMPP
Federation

TRANSPORTS & MESH NETWORKING

TCP/IP, HTTP, Wireless, Sneakernet

Rhizome

Zyre

BATMAN etc

OPERATING SYSTEM

Reproducible Build & Trust Chain

EthOS

gentoo / libertè linux
debian / TAILS / whonix
cyanogenmod / *BSD

freedombox

Apple

Microsoft
Google

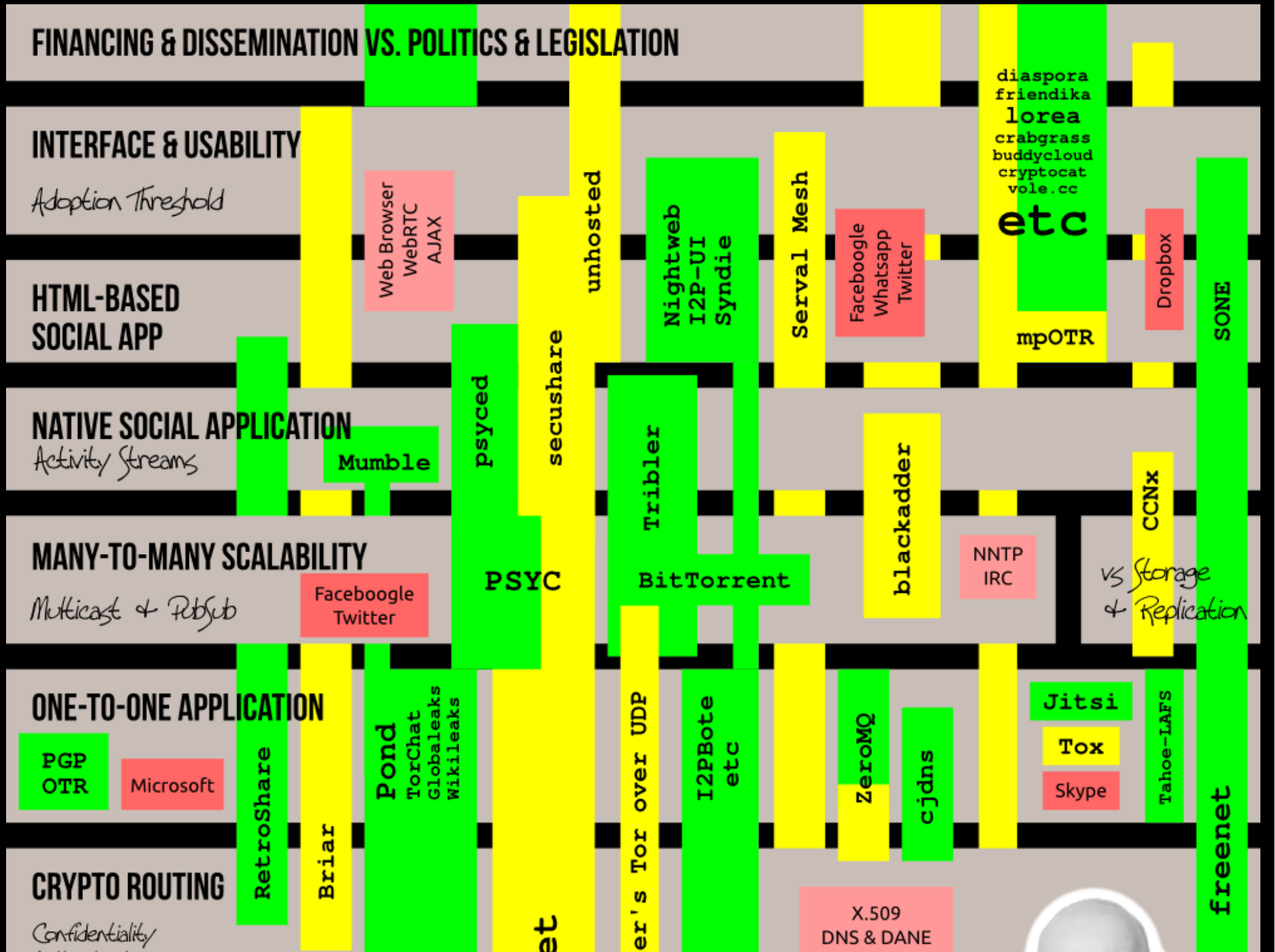
FREE HARDWARE

MilkyMist

novena

intel &
others

intel AMT


FINANCING & DISSEMINATION VS. POLITICS & LEGISLATION
INTERFACE & USABILITY
Adoption Threshold
HTML-BASED SOCIAL APP
NATIVE SOCIAL APPLICATION
Activity Streams
MANY-TO-MANY SCALABILITY
Multicast & PubSub
ONE-TO-ONE APPLICATION
CRYPTO ROUTING
Confidentiality
Web Browser
WebRTC
AJAX
unhosted
Nightweb
I2P-UI
Syndie
Serval Mesh
Faceboogle
Whatsapp
Twitter
diaspora
friendika
lorea
crabgrass
buddycloud
cryptocat
vole.cc
etc
mpOTR
Dropbox
SONE
Mumble
psyced
secushare
Tribler
BitTorrent
blackadder
NNTP
IRC
CCNx
vs Storage & Replication
Faceboogle
Twitter
PSYC
PGP
OTR
Microsoft
RetroShare
Briar
Pond
TorChat
Globaleaks
Wikileaks
I2PBote
etc
ZeroMQ
cjdns
Jitsi
Tox
Skype
Tahoe-LAFS
freenet
X.509
DNS & DANE


SECURE
SHARE