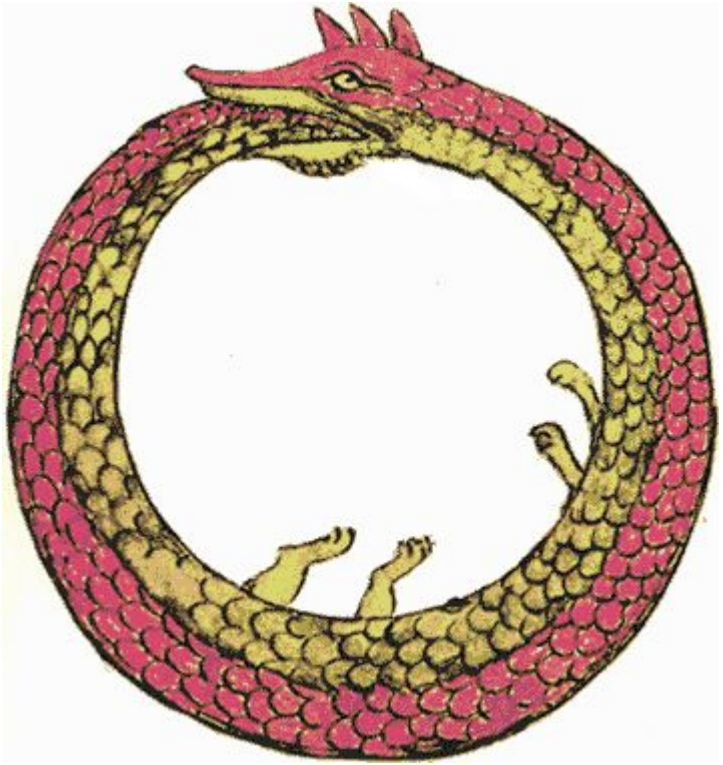
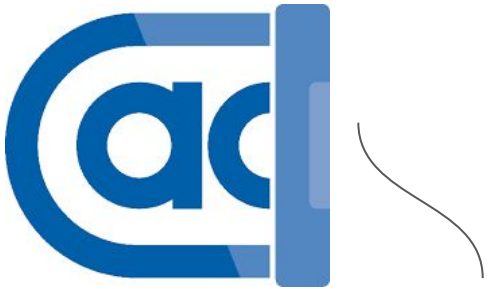
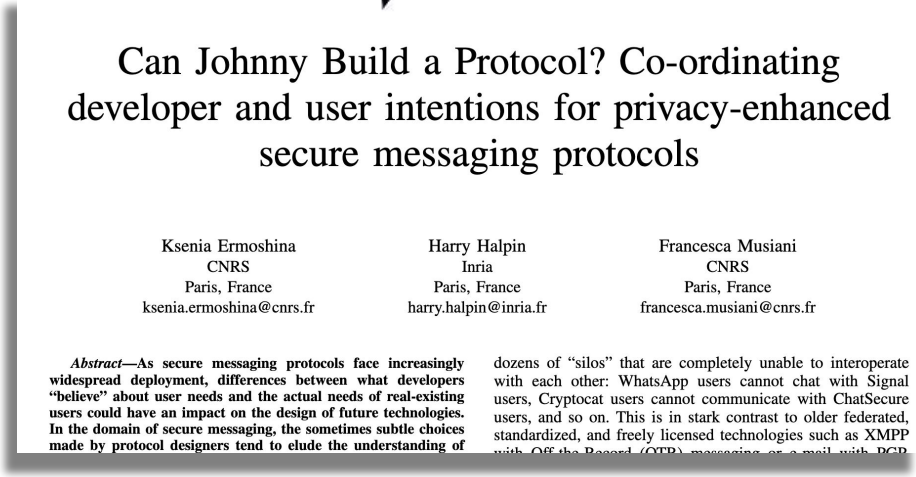
Always more secure?

Understanding user migrations to federated platforms



A “useful sociologist”?





Can Johnny Build a Protocol? Co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols

Ksenia Ermoshina
CNRS
Paris, France
ksenia.ermoshina@cnrs.fr

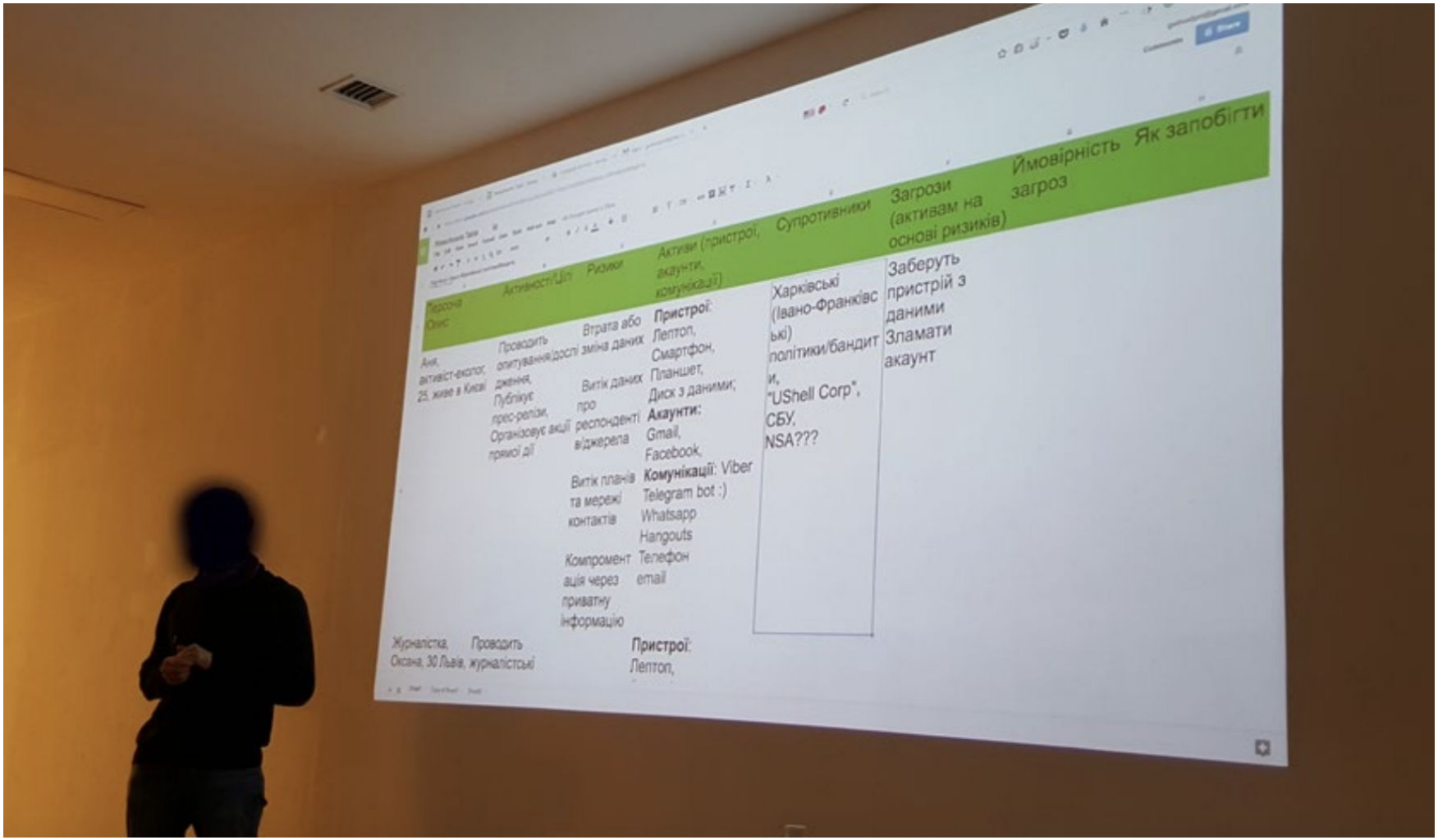
Harry Halpin
Inria
Paris, France
harry.halpin@inria.fr

Francesca Musiani
CNRS
Paris, France
francesca.musiani@cnrs.fr

***Abstract*—As secure messaging protocols face increasingly widespread deployment, differences between what developers “believe” about user needs and the actual needs of real-existing users could have an impact on the design of future technologies. In the domain of secure messaging, the sometimes subtle choices made by protocol designers tend to elude the understanding of**

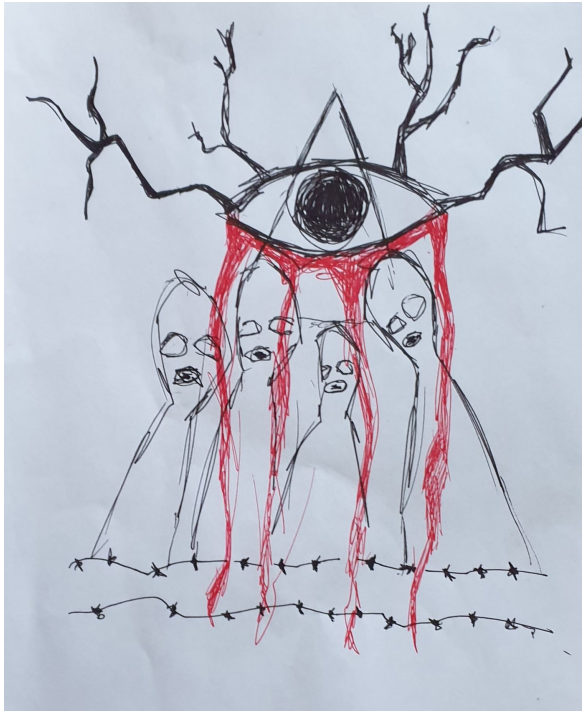
dozens of “silos” that are completely unable to interoperate with each other: WhatsApp users cannot chat with Signal users, Cryptocat users cannot communicate with ChatSecure users, and so on. This is in stark contrast to older federated, standardized, and freely licensed technologies such as XMPP with Off-the-Record (OTR) messaging or e-mail with PGP

nextleap.eu

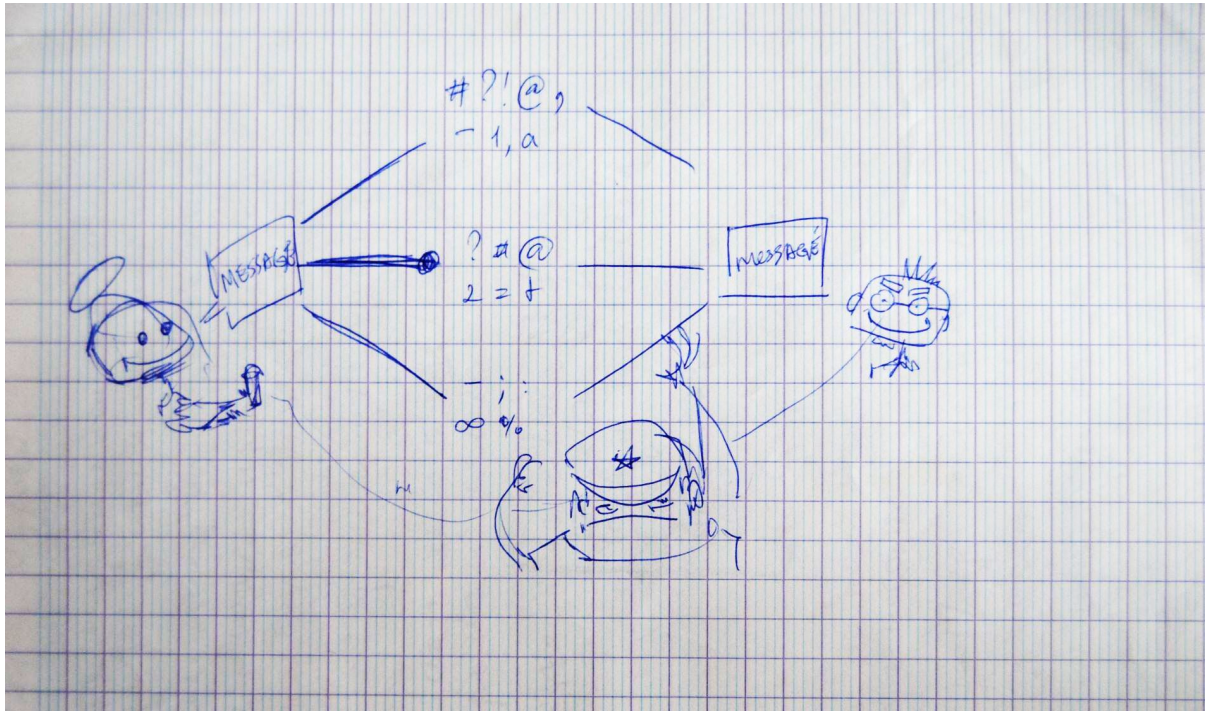

Персона
Опис
Активності/Цілі
Ризики
Активи (пристрої, акаунти, комунікації)
Супротивники
Загрози (активам на основі ризиків)
Ймовірність загроз
Як запобігти
Ані, активіст-еколог, 25, живе в Києві
Проводить опитування/дослідження, Публікує прес-релізи, Організовує акції прямої дії
Втрата або зміна даних
Витік даних про респонденті відджерела
Витік планів та мережі контактів
Компромент ація через приватну інформацію
Пристрої: Лептоп, Смартфон, Планшет, Диск з даними; Акаунти: Gmail, Facebook, Комунікації: Viber Telegram bot :) Whatsapp Hangouts Телефон email
Харківські (Івано-Франківські) політики/бандити, "UShell Corp", СБУ, NSA???
Заберуть пристрій з даними Зламати акаунт
Журналістка, Оксана, 30 Львів,
Проводить журналістські
Пристрої: Лептоп,

“Fears and hopes of the Internet”: 120 drawings collected; ongoing study

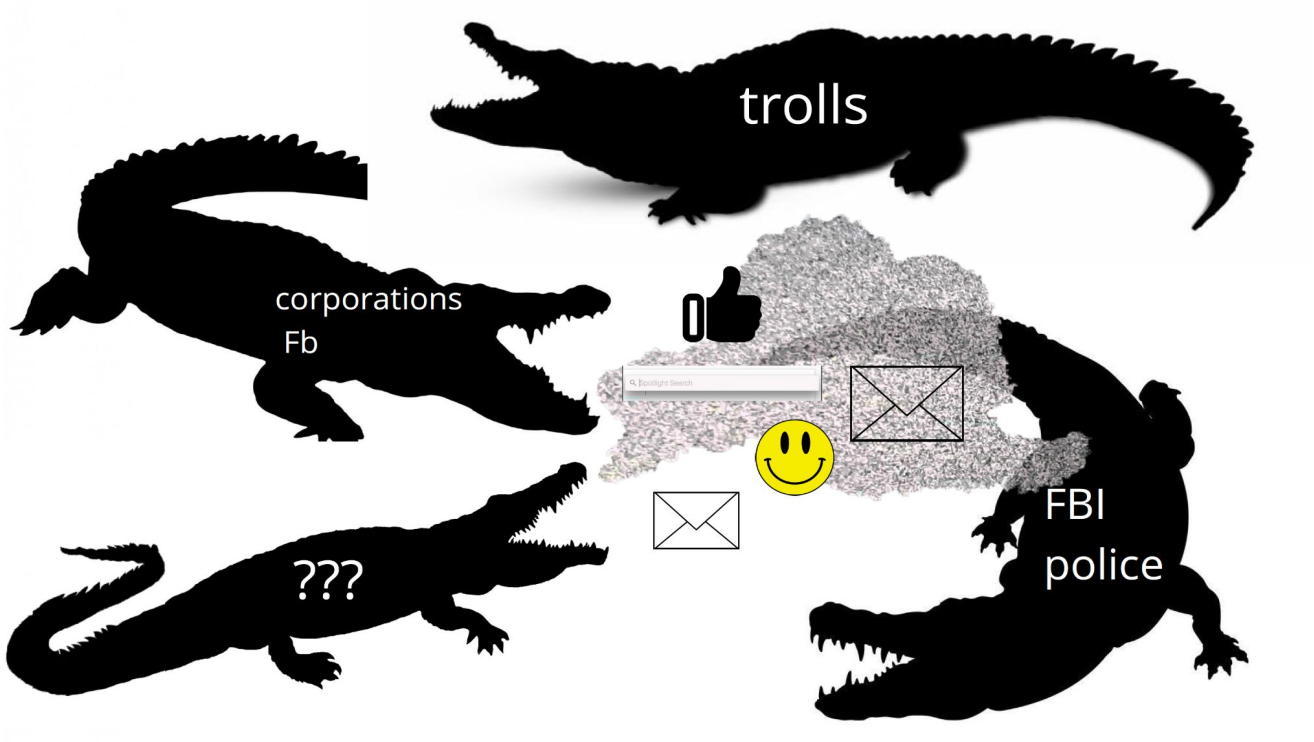
Fears: from a central threat to a continuum of threats



Fears: from a central threat to a “threat continuum”



Fears: from a central threat to a continuum of threats



Fears: from a central threat to a continuum of threats

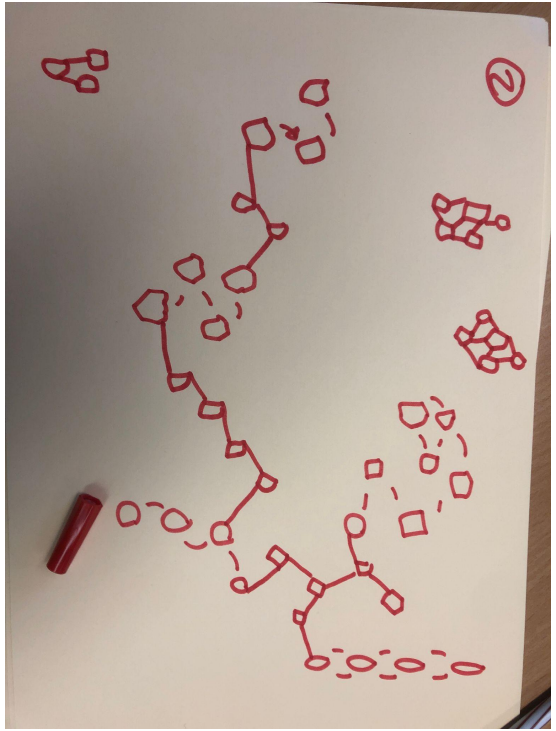
Interview	Developers	Low-risk Users	High-risk Users
Number	15	18	15
Repudiation (Security)	high	low	low
Group Support	high	high	high
Metadata Collection (Privacy)	high	low	high
Decentralization	high	low	low
Standard	high	low	low
Open Licensing	high	low	low

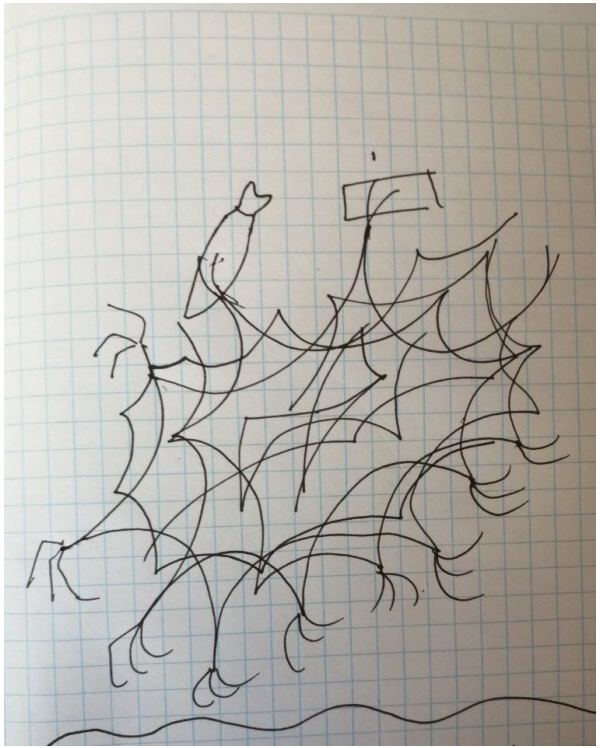
TABLE II. IMPORTANCE OF PROPERTIES OF SECURE MESSAGING INTERVIEWS

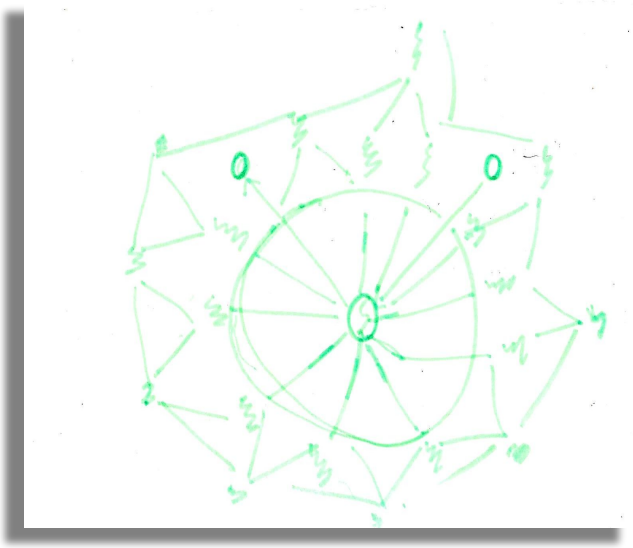
YES, BUT…

DECENTRALIZATION MATTERS!

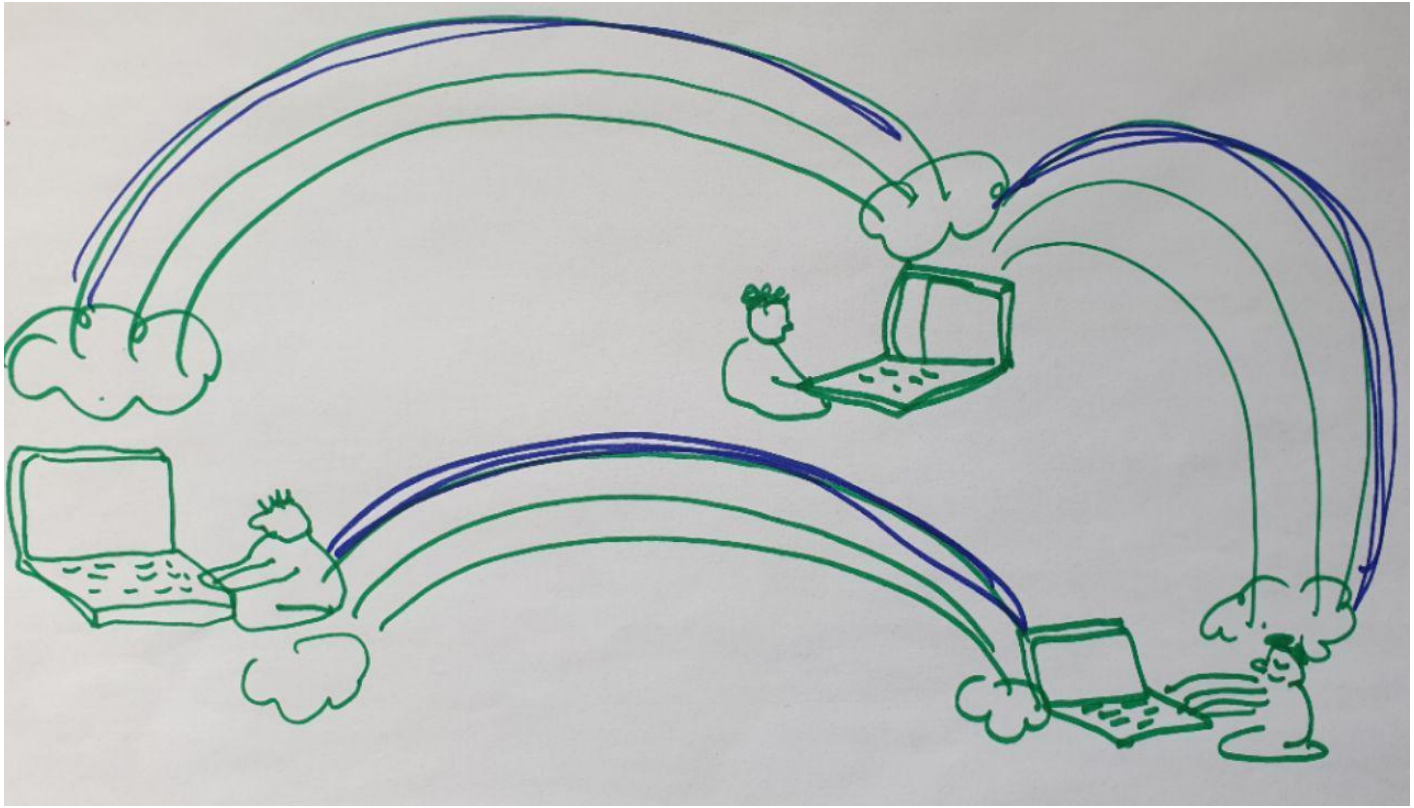
An “ideal Internet” looks like…



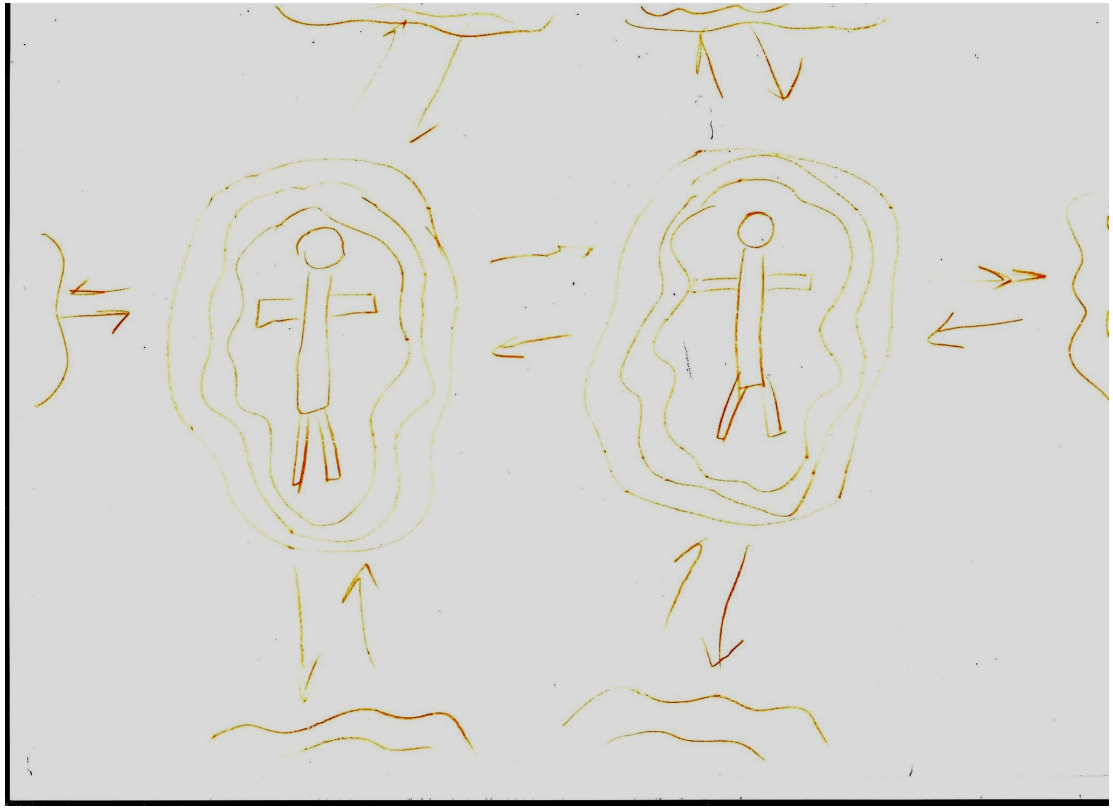




An “ideal Internet” looks like…

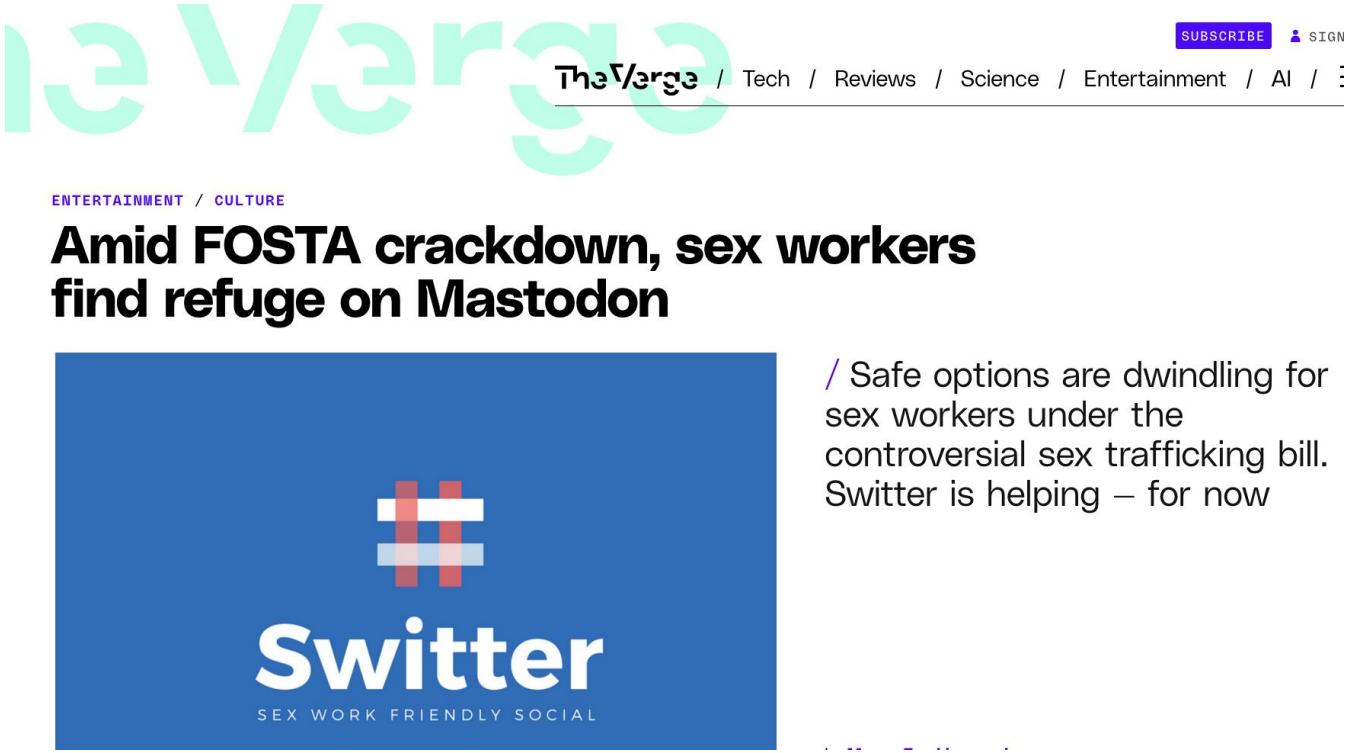


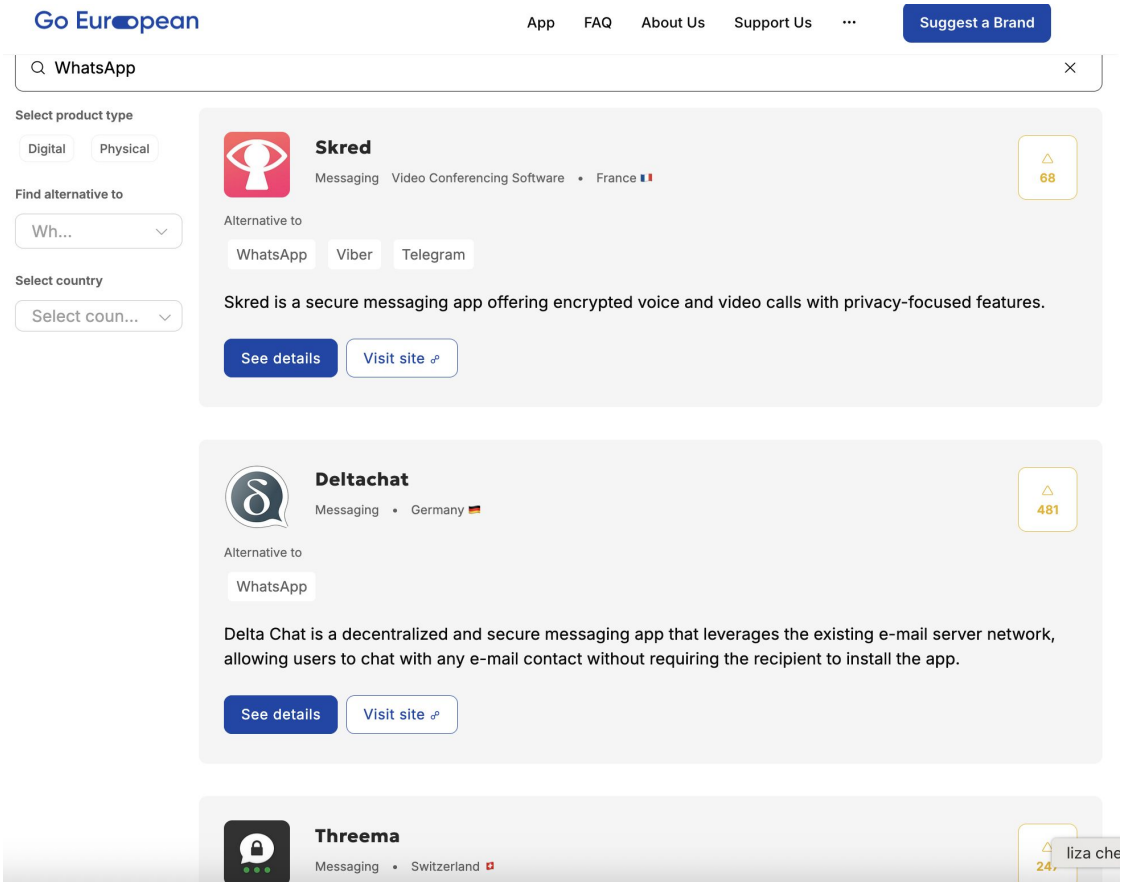
An “ideal Internet” looks like…



Migrations to the Fediverse… not so new!

Waves of migrations: from marginalized users…





…to European public sector

A “federated sovereignty”?

“From a geopolitical perspective, the risk for decentralized countries in Europe comes from large, centralized authoritarian superpowers. A decentralized communication system is therefore necessary to enable coordination while maintaining sovereignty, and to compete with a centralized top-down approach mandated by competition” (Matthew Hodgson, interview, March 1, 2025)

But what about that old debate?

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 past four years. We want to share some of the thin we've learned while doing it.

Moxie Marlinspike on Decentralization

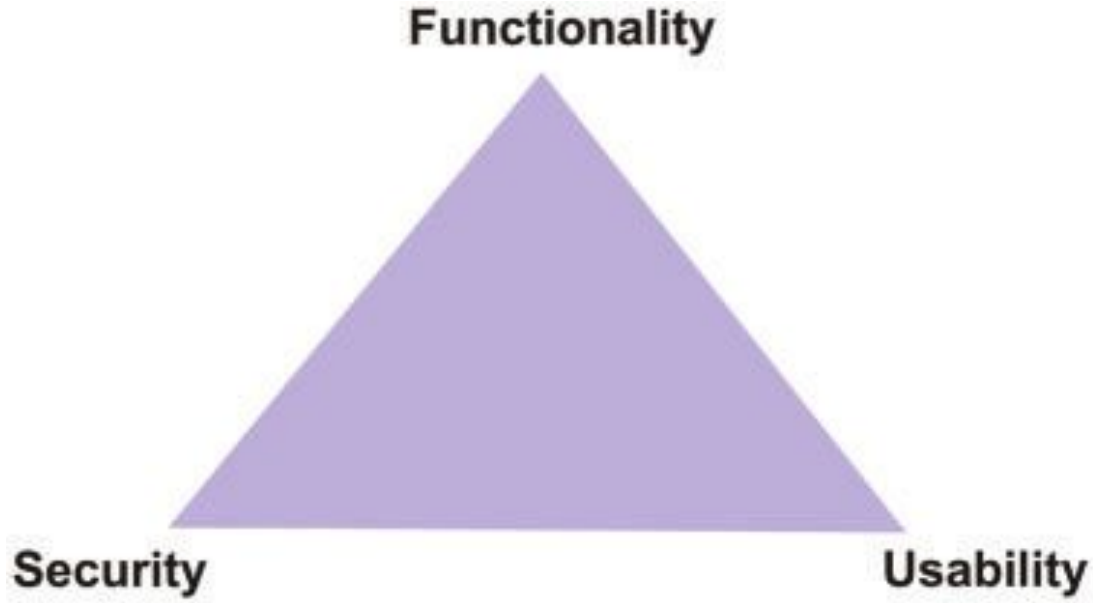
Moxie Marlinspike, founder and former CEO of Signal Messenger LLC, on the topic of decentralization and why centralized systems are supposedly the way to go.

Home / Software / Standardization / Posts

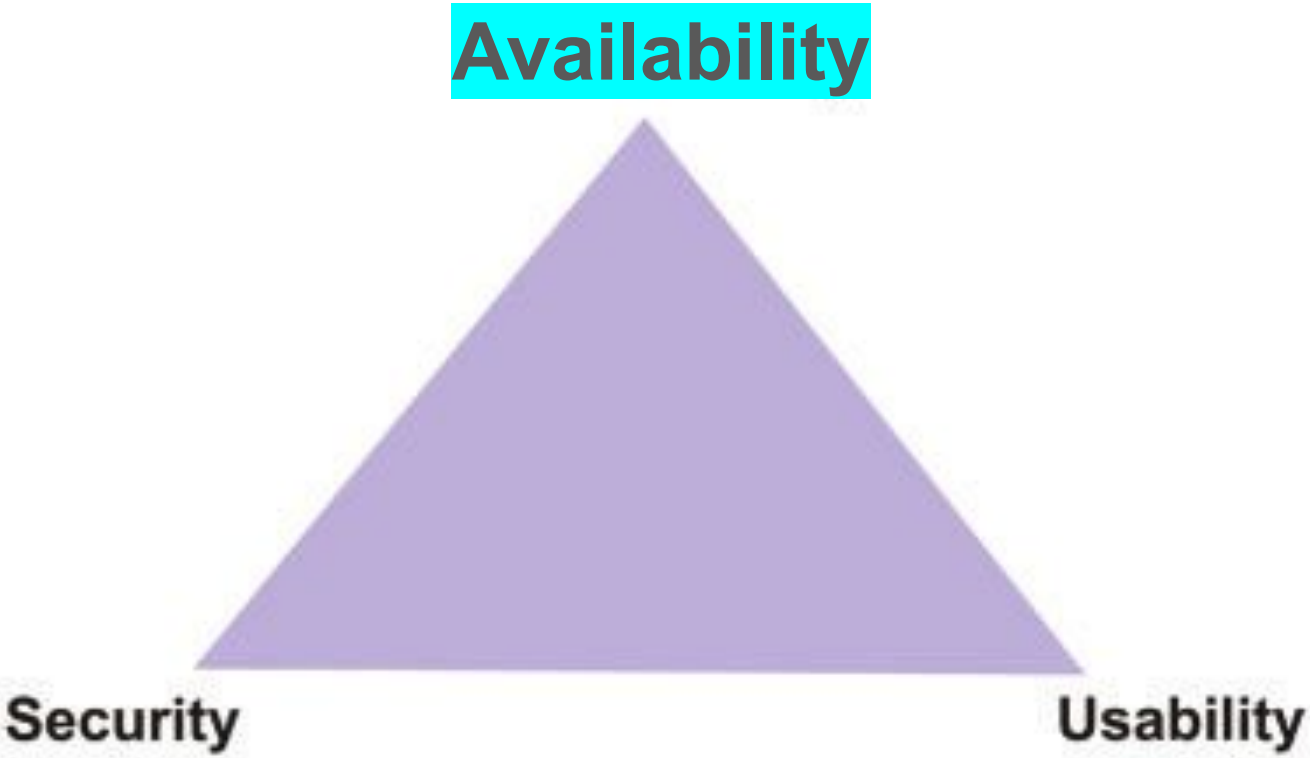
AN OBJECTION TO 'THE ECOSYSTEM IS MOVING'

November 30, 2016 / 5 minutes

In May 2016 Moxie Marlinspike published an article on his company's blog entitled 'Reflections: The ecosystem is moving' where he claims that federated systems are 'stuck in time'. Since then his blog post has been passed around primarily to support the argument that federated, XMPP based, instant messaging is not working and won't ever provide a decent user experience. On the other hand his blog post is rarely used as an argument on how bad the World Wide Web is and on how we should all give up on using the Web, even though HTTP is one of the protocols Moxie claims to be stuck in time. In fact Moxie picks his examples very carefully and only talks about



Source: Attaallah, Khan, 2021


Availability
Security
Usability

Resilience is key

- When nothing works, people fall back to unsecure alternatives (see Ermoshina, Musiani, 2024)
- Infrastructural dependencies of centralizes solutions may lead to fails in critical situations

Signal mostly blocked in Russia #7745

Closed

Jump to bottom

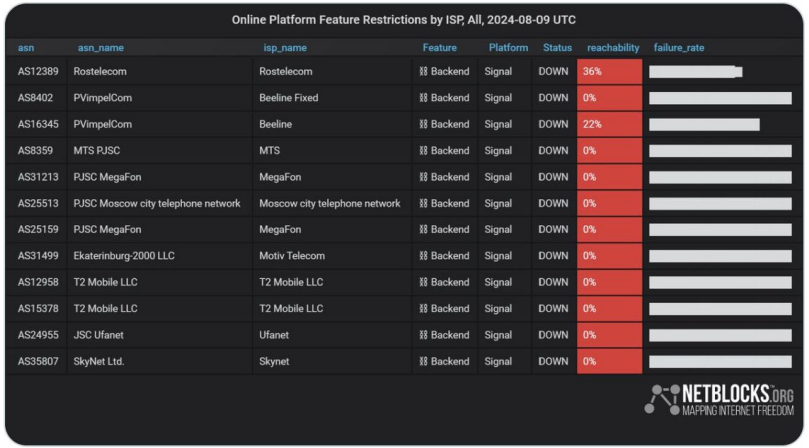
leedoyle opened on Apr 28, 2018 · edited by leedoyle

Edits

Due to Roskomnadzor action against Amazon and Google networks used by Telegram to circumvent its ban in Russia (method previously used by Signal in other countries), most of Signal's functionality is blocked, at least for large ISPs. Currently, only **basic text messaging is possible** - without voice messaging, video or photo sharing(photo and video sharing may still work for some ISPs) .

NetBlocks @netblocks

⚠️ Confirmed: Metrics show #Russia has restricted Signal messaging app backends on most internet providers; regulator Roskomnadzor states that the ban has been imposed to prevent Signal's use for "extremist" purposes; the app remains usable with "censorship circumvention" enabled

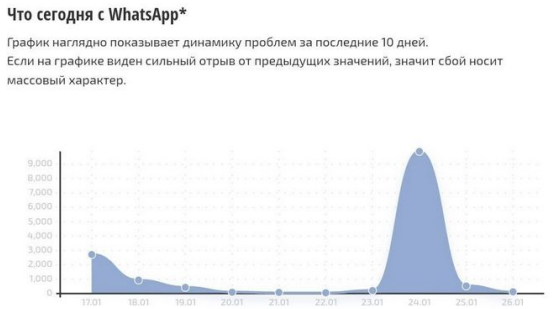


Michael Klimarev

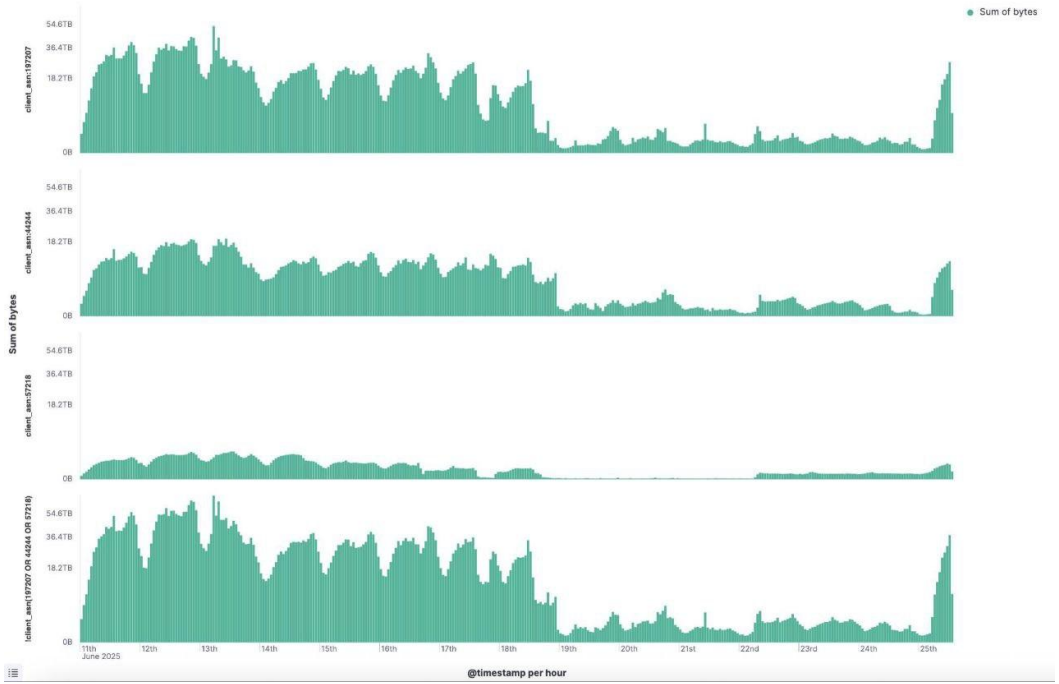
Local and regional shutdowns, new throttling practices

Ingushetie, 2018:

Bashqortostan, 2024:



Iran, 2025



Right now DeltaChat is working great in Iran's Internet blackouts too. Great job.

۰۱ تیر ۱۴۰۴، ۱۵:۲۲ · Pachli

۱۳ تقویت · ۲۰ برگزیده

ag1km
ag1km@mastodon.social@

۱ تیر

hosein@ delta@ I guess you are using a local mail provider, right? Not the default one from delta chat?

۱

حسین
hosein@

۱ تیر

ag1km@

True, I set up a chatmail.at server on a VPS in Iran.

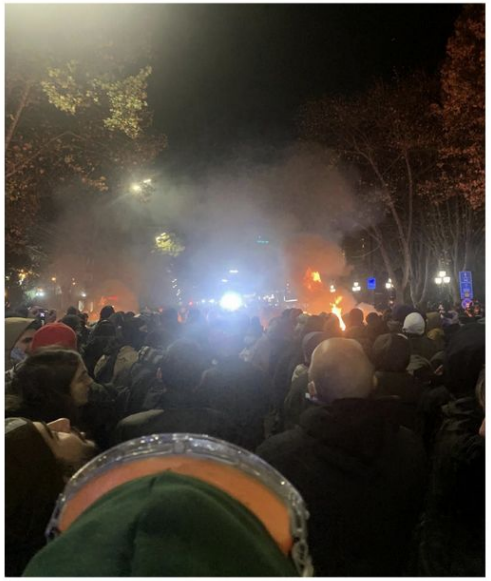
I have also provided my users with binary files of delta chat since the app markets like Google Play and F-Droid vanish too.

I'd like to thanks delta@ once again, not only for the apps' great user experience, the ability to self-host, and the amount of privacy my users now have on my servers, but also for their dedication to help people. I just asked them some questions in DMs and they have been very helpful.

From labs to forests and streets

Kyiv, Ukraine, 2018

Forest, St Petersburg, Russia, 2020



Tbilisi, Georgia, 2024

Decentralization means a lot of things

- Infrastructural decentralization → growing local
- Social decentralization → not dependent on “charismatic leaders” (e.g. Monsieur Pavel Du Rove)
- Users identities are decentralized
- Financial decentralization → going away from US fundings
- Some centralized apps are also decentralized in a weird way (e.g. Signal depending on multitude cloud providers)