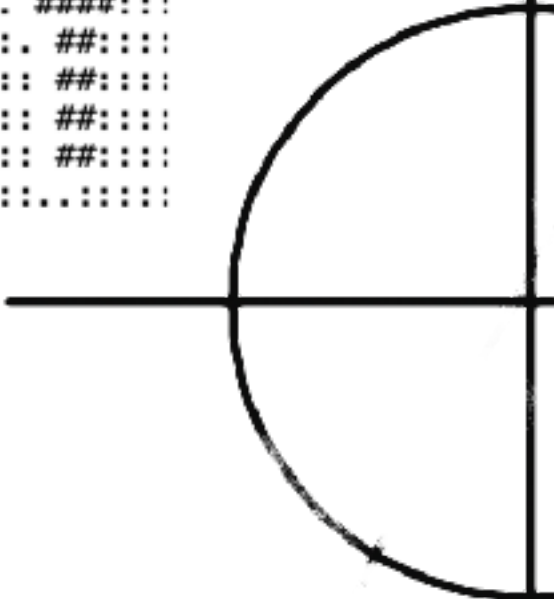


```

#####: ::: '###: ::: '#####: ::: '#####: '##: ::: #: '#####: '##: ::: '##:
##. . . . ##: ::: '## ##: ::: '##. . . . #: #: . . . . : ##: #: '##. . . . #: . #: '##:
##: ::: #: '##. #: #: : . . . : #: : : : #####: #: #: : . . . : . #####:
#####: '##: ::: #: #: : '###: #####: #: ## #: #: : : : . #: :
##. . . . : #####: ##: #: #: . . . . : ##. #####: #: : : : #: :
##: : : : #: . . . #: #: : #: : #: : #: : #: : #: : #: : #: :
##: : : : #: : #: . #####: #####: #: . #: . #####: : #: :
. : : : . : : : . : : : . : : : . : : : . : : : . : : : . : : :

```



Privacy-enhancing web3 use-cases ideation framework

Web3 tech stack could empower human privacy

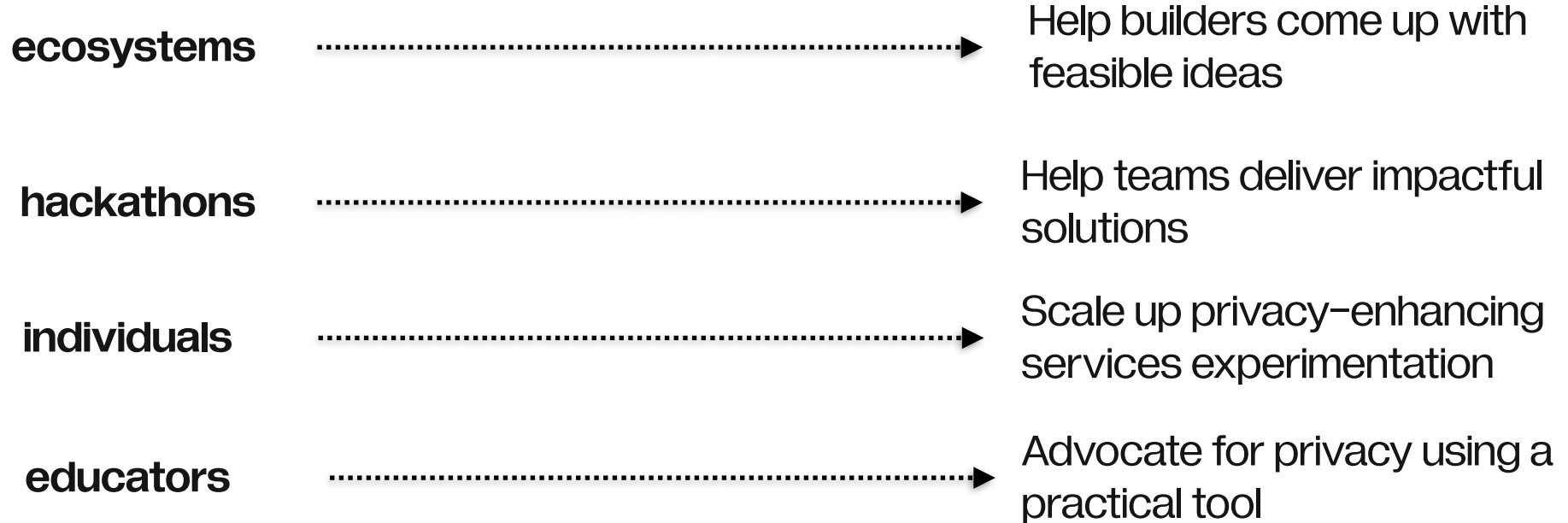
Raise awareness about the necessity of privacy protection.

Build tools to enhance privacy.

Advocate for the following business models not based on surveillance capitalism.

Return human agency for data-driven decision making.

Audiences



The more use-cases would be shipped ->
the better Web3-privacy would progress as a habit, lifestyle & basic human right.

##

FRAMEWORK

Humans



Data



Challenge

Resources



Success metrics

Threat agents

Partners



Solution



Privacy layers





Who are you building for?
Why should they care?

Create in-depth human-personas based on interviews or research.

Web3 services usage

- What kind of web3 services this human uses?
- What are the data breaches in those services?

Personal data literacy

- Does a person know how his/her/theirs data has been abused?
- Does a person know how to protect himself/herself/themselves?
- What kind of privacy-enhancing solutions does a person use?



Privacy

- How aware is a person of the necessity for privacy protection?
- How easily person would give up privacy in exchange for services or product features?
- Why this human needs privacy protection?
- What would happen with a human without additional privacy?

Empathy

Try to talk with some of those people. Talk broadly about their internet rights, privacy, web3 services, and security. Make products for them & not just for yourself.

Suggestions

- Web2 users** - help them to convert to Web3
- Web3 users** - empower their existing services

Hint: focus on humans as communities, not just individuals.



What kind of data are you protecting?

Why does this data matter?

Write down a list of sensitive data you aim to protect or re-design business model.

Data is the fuel of blockchain & surveillance capitalism. It's regularly exploited & used by third parties without your consent. Not just Google or Facebook, but also Web3-services from wallets to CEXs collect personal data.

Exploited data could be presented in different forms:

- transactional data
- IP addresses
- name
- age
- geo
- wallet address etc

Example

Google services track your online behaviour, make look-alike modelling & sell your profile to advertisers. So you become "a product".

References

Data brokers [description](#)

Facebook-Cambridge Analytica [case](#)

Suggestions

- Explore how Data flows within the internet.
- Explore how Data brokers collect & sell sensitive data.
- Explore how Web2 & Web3 data correspond with each other.
- Analyse how much Data you share with third parties daily.

Hint: think of both on-chain & off-chain data when you are doing research.



What are the main barriers on your way?

How do they compromise the person, you, industry?

Write down a list of challenges that stand between humans & your idea.

Web3 isn't a transparent or regulated market. That's why it's easier to spy on humans. At the same time, humans don't know how to choose the correct privacy-enhancing service.

Examples

- unregulated blockchain-data aggregation
- third party surveillance
- lack of privacy literacy
- "fake privacy" within existing solutions
- existing architecture allows third parties to spy on personal data

Suggestion

Analyse the Tornado Cash case from open-source development & DAO governance perspectives.

Hint: think of the ZK market that solves the challenge of preserving sensitive data while validating parts from KYC to age verification.

NAME	AGE	SEX	HEIGHT	WEIGHT	HAIR	EYES	ETHNICITY	RELIGION	POLITICAL	IDEOLOGY	ACTIVITY	STATUS
John	25	M	180	75	Brown	Blue	White	Christian	Conservative	Liberal	Active	Single
Jane	30	F	165	60	Blonde	Green	Black	Muslim	Liberal	Conservative	Inactive	Married
Mike	40	M	175	80	Black	Brown	Hispanic	Buddhist	Conservative	Liberal	Active	Married
Sarah	28	F	170	65	Red	Blue	White	Christian	Liberal	Conservative	Active	Single
David	35	M	185	70	Black	Blue	White	Christian	Conservative	Liberal	Active	Married

Who is threatening privacy-balance?

How do these bad actors use personal data?

Write down a list of multiple actors challenging web3 privacy from the data-analytics companies to marketing agencies.

Specify what threats these actors cause: selling, spying, stealing data etc.

Examples

Corporations – Google is at the heart of surveillance capitalism, selling humans’ data to advertisers.

Hackers – exploit vulnerabilities in tech, sell databases with personal data.

Scammers – malicious actors behind stolen funds.

Governments – think of the [NSA](#) or [Pegasus](#) cases dealing with gov surveillance apparatus.

Dara brokers – specialises in collecting personal data or data about companies, mostly from public records but sometimes sourced privately, and selling or licensing such information (Experian, Equifax, Acxiom).

References

- Chainalysis used the block explorer website to collect wallets & other data: [click](#)
- ConsenSys revealed that it collects user data: [click](#)

What would web2 do:

Hint: actors could be both web2 or web3 native.



What privacy layer are you contributing to?
What's a trade-off compared to other layers?

Choose one of the different approaches to the web3 privacy-enhancing: from embedded to total anonymity. The approach depends on compliance-readiness & moral beliefs.

Definitions

Embedded – network-level privacy that allows seamlessly deploy privacy within dApps. Privacy by default.
Example: [Manta Network](#)

Configurable – is a configurable approach to privacy that lets humans disclose their transactions to third parties.
Example: [Aztec](#)

Enterprise ready – enterprise grade & government compliant privacy protection standard.
Example: [NYM](#)

Total anonymity – human-centric privacy without compliance compromises & invisible to law enforcement units.
Example: [DarkFi](#)

Resource: Web3 privacy layers overview from embedded to total anonymity [article](#)

Hint: think of a privacy implication complexity: KYC+AML could be great for accountability in the USA, but it means the death penalty in Iran

How your idea empower humans?

How sustainable is your solution in 1-3-5 years?

Brainstorm the bravest ideas without the limits.
Then, visualise them using traditional or digital surfaces.

Apply the following filters to choose idea you like the most:

Privacy-first: it's in line with privacy-enhancement

Usable: it's easy to use &/or implement

Empowering: it empowers humans' lives

Impactful: it shapes existing surveillance vs privacy balance

Feasible: it's possible to develop an idea from tech, open-source & economic points

Examples (web3-native)

- dVPN hides your actual IP address from third party websites & apps
- Messengers protect your private communication from exploitation
- Private currencies could protect human identity in front of oppressive government

Hint: lots of web3 solutions complement each other - an ecosystem-centric approach simplifies ideation/development

##

What partners could scale your idea?

What kind of value do these partners add?

Write down actors that could help you to activate or scale the solution.

Make reverse engineering: imagine a time when your solution has been implemented on a broader scale. What kind of partners do you need to make this happen?

Examples

Investors – cover development & marketing costs, scale up market delivery

Developers – implement & adapt the solution to speed up Product-market-Fit

Institutions – could advocate & adopt solutions (think of messenger like Signal here).

Journalists – they could become ambassadors of your solution

Opinion Leaders – both traditional or web3's best actors preaching for change (from Vitalik to Shoshana Zuboff)

Hint: partners should unlock value for you

#####

What resources do you need for a start?

What resources do you need to sustain your idea (1-3 years)?

Write down all potential resources you need to launch your idea & sustain it.

Split idea implementation into phases: MVP, Product-market-Fit, Scaling.
Each phase requires a different amount of resources.

Examples

- Financial expenses
- Human resources
- Partners
- Legal support
- Investments
- Community
- Governance

Suggestions

- Think broadly about missing skills from the team (example: developer doing investment relations).
- Think about the potential business model (grants, sponsorships, subscriptions, fees etc)

Study
How Rotki is trying to find the Product-Market-Fit [being open-source](#) + [Gitcoin](#)

Hint: resource management could come in handy, helping to understand feasibility of idea for yourself & wider audiences (from hackathon jury to investors)

Agency framework template

Humans

Create in-depth human-personas based on interviews or research.

Data

Write down a list of sensitive data you aim to protect or re-design a business model for.

Challenges

Write down a list of challenges that stand between humans & your idea.

Resources

Write down all potential resources you need to launch your idea & sustain it: money, community support, media coverage, legal, ecosystem activations (development relations, business development).

Success metrics

Write down a list of metrics that define the success of the product.

Threat actors

Write down a list of multiple actors challenging web3 privacy from the data-analytics companies to marketing agencies. Then, specify what threats these actors cause: selling data, spying etc.

Partners

Write down actors that could help you to activate or scale the solution. They could be developers, web3 companies, investors, media & even institutions.

Solution

Brainstorm the bravest ideas without the limits. Then, visualise them using traditional or digital surfaces.

Privacy layers

Choose one of the different approaches to the web3 privacy-enhancing: from embedded to total anonymity. The approach depends on compliance-readiness & moral beliefs.

Agency framework implementation

Simplified to do list to follow

- 1. Humans.** Create in-depth human-personas based on interviews or research.
- 2. Data.** Write down a list of sensitive data you aim to protect or re-design a business model for.
- 3. Challenges.** Write down a list of challenges that stand between humans & your idea.
- 4. Threat actors.** Write down a list of multiple actors challenging web3 privacy from the data-analytics companies to marketing agencies.
- 5. Solution.** Brainstorm the bravest ideas without the limits. Then, visualise them using traditional or digital surfaces.
- 6. Partners.** Write down actors that could help you to activate or scale the solution. They could be developers, web3 companies, investors, media & even institutions.
- 7. Resources.** Write down all potential resources you need to launch your idea & sustain it: money, community support, media coverage, legal, ecosystem activations (dev & business relations)
- 8. Success metrics.** Write down a list of metrics that define the success of the product.

Principles of privacy-enhancing development

Human centered

.....

Place humans in the centre of your idea. Care about his/her/theirs emotions, crypto & privacy literacy.

**Solve an actual
privacy-specific problem**

.....

Empower humans with practical privacy solutions that could be used here & now.

**Accessible to
the future Web3 audience**

.....

Think about newcomers using your services in forthcoming years.

Ethical

.....

Don't build services for money laundering, criminal activities or violating human rights.

Open-source

.....

Make your idea accessible to the world via GitHub, Devfolio, GitLab.

Idea valuation

Default state: Decentralisation ethos sync – it redistributes power from centralised actors back to humans.

Problem Importance

How important is the problem being solved? (10: extremely important)

Privacy-solution impact (addressable market)

> thousands, millions

Ease of implementation

How complex is the implementation: budget, team, processes > from 1 to 10

Effectiveness

How effectively does the idea address the referenced problem? (10: ultimate effectiveness)

Product-market-Fit

time vs efficiency

Community contribution

re-usability, compostability

##

##



Humans

People who are using web2 browsers (Chrome, Firefox)

Affected by surveillance capitalism, but without knowing that they are exploited.

Low privacy literacy (different privacy culture: high in the EU, low in underdeveloped countries)

Resources

People: MarTech experts (surveillance tech), copywriter, UX/UI designer, business development manager...

Investors (\$100K for an MVP launch)

1 year operational budget (salaries, events, community outreach)

Partners

Investors: strategic investors with access to big web2 audience (for example, via DuckDuckGo or ProtonMail)

Journalists: web2 tech journalists
Civic tech advocates: institutions or influencers

Data

Browsing data (websites, web-services, time, geo, IP, usage; social profiling).

Cookies

Success metrics

Product: trackers prevention rate

People: ease of use, understanding of privacy-centric product, conversion rate from web2 to web3 browser

Open-source: ease of fork, ease of pull requests

Solution

Native web3 browser that protects user private data & prevents them from reach marketing tracking.

Zero-personal data aggregation policy.

Challenges

Human-centric

Low lever of privacy awareness.

Low level of tracking awareness.

Low level of Web3 services understanding.

Threat actors

Corporation from Google to Facebook. MarTech services.

Advertising agencies.

Privacy layers

Embedded privacy – “as a service” to person, “hidden as a service”, but explicit via communication and/or proofs.

Access layer (browsing web2 websites).



Humans

People, who are using existing Ethereum wallets (MetaMask, BlockWallet etc).

Primary audience: people familiar with privacy, but with lack of knowledge how to protect themselves (can't setup their own RPC, use VPN).

All genders, English speaking.

Secondary audience: opinion leader obsessed with privacy, tech literate.

Resources

People: copywriter, UX/UI designer...

Investors: angel investors, ecosystem labs/funds

Partners

Investors: strategic investors with access to huge crypto-native audience

Journalists: crypto journalists

Crypto influencers: Ethereum influencers (devs, Ethereum Foundation team, Vitalik)

Data

IP addresses, wallet addresses – available wallets do not protect users' sensitive personal data

Challenges

Convince people to switch from non-private or semi-private to full-private solution.

Raise awareness about privacy level within the wallets solutions.

Manage Tor connections

Success metrics

Product: proven Trustless architecture (within independent opinion leaders)

Experience: ease of use, high consent of the privacy-centric solution, conversion rate from other wallets to Lunar

Open-source: ease of fork, ease of pull requests

Threat actors

Available wallets do not protect users' sensitive personal data.

Third parties: RPCs (Infura, Alchemy), Coingecko, Etherscan, CoinMarketCap...

Wallet servers (BlockWallet) and third parties servers are able to link users' IP addresses and wallet addresses.

Solution

The first privacy native Ethereum wallet based on a **built-in integration of TOR**. This architecture enables users' IP addresses to be isolated from third parties.

Trustless architecture – the user does not need to trust the wallet regarding his personal data as the wallet's third parties cannot see or share its users' IP addresses.

Privacy layers

Embedded privacy – “as a service” to person, “hidden as a service”, but explicit via communication and/or proofs.

Access layer (managing cryptocurrencies).

##

Useful materials

Lectures

Kurt Opsahl “The value of cryptocurrencies in supporting of human rights”: [watch](#)

Jaya Brekke (CSO, NYM) “Privacy, the big picture”: [watch](#)

Web3 privacy-enhancing projects

Web3privacy now database: [explore](#)

Web3 privacy landscape [map](#)

Books

Shoshana Zuboff “The Age of Surveillance Capitalism”: [buy](#)

Rebecca Giblin and Cory Doctorow “Chokepoint Capitalism”: [buy](#)

Hackathons

ETH Brno [privacy & security edition](#) + [Devfolio](#)

Press

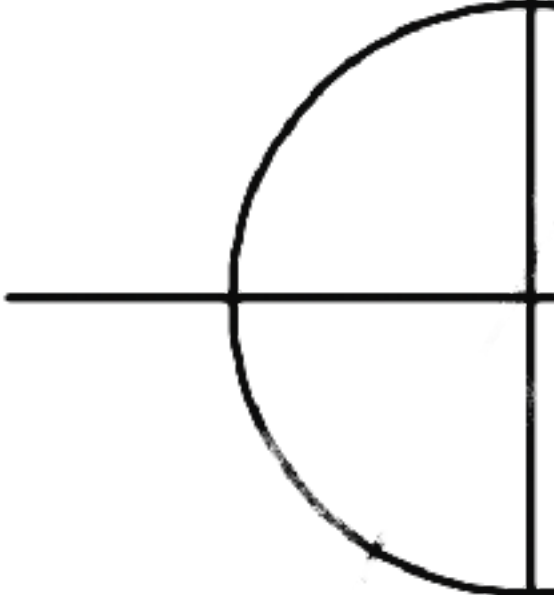
Coindesk Privacy week [materials](#)

Movies

[The Social Dilemma](#)

Activate privacy as 1-2-3,

#####:':###:'::#####:#####:##:':###:':###:':###:
##... ##:':## ##:':##... ##:##.....:###:##:##... ##:##:###:
##:':###:##:##:':###:###:###:###:###:###:###:###:###:###:
#####:###:':##:###:#####:### ## ##:###:':###:###:###:
##.....:#####:##:':##:##.....:##.###:###:###:###:###:###:
##:':###:##... ##:###:##:###:###:###:###:###:###:###:###:
##:':###:###:###:#####:#####:##:':###:###:#####:###:###:
.....:':###:###:###:###:###:###:###:###:###:###:###:###:###:



web3
privacy
now

Mykola
Siusko, 2022

Contribute  [Web3privacy now](https://github.com/Web3privacynow)
Connect  [@nicksvyaznoy](https://twitter.com/nicksvyaznoy)