Antonios Hazim

Human Centered Privacy Design

Privacy Visualizations & Privacy by Design in FOSS

Plan

I. Privacy Visualizations in F-Droid
    I. The Problem
    II. Procedure
    III. Results & Insights
II. Privacy by Design Guidelines for FOSS
    I. The Problem
    II. Procedure
    III. Insights
III. Issues & Future Work

Context: Privacy & Software

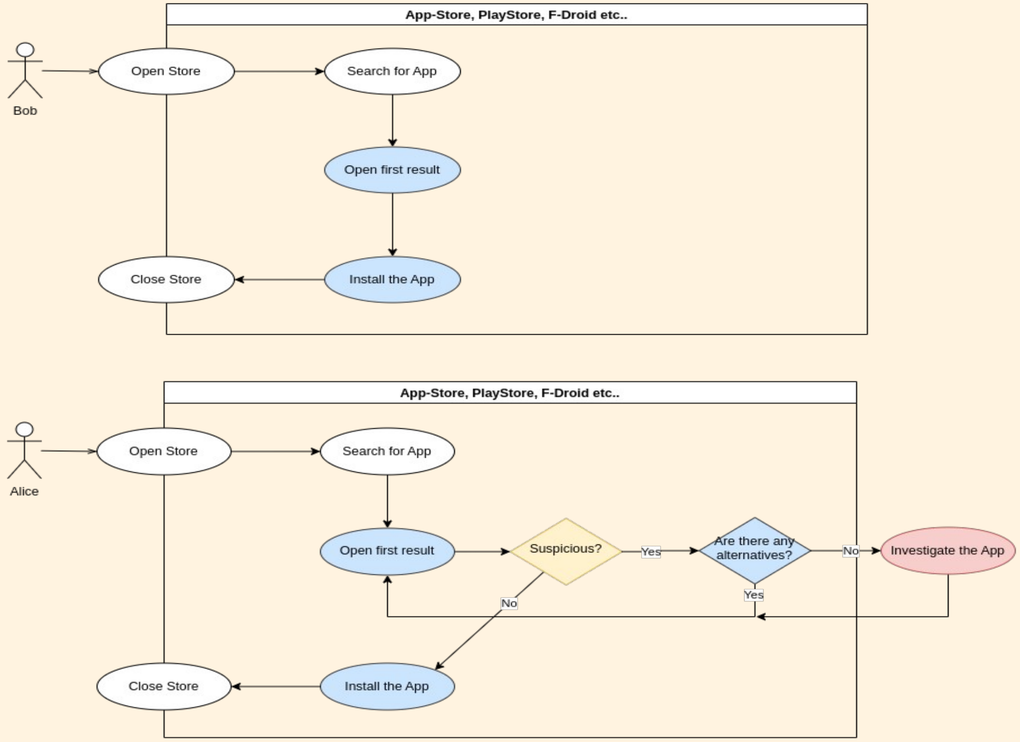
- **Privacy Visualizations**

  - User-facing aspect
  - Design with Focus on UX
  - Mainly from UX researches

- **Privacy by Design Guidelines**

  - Developer-facing aspect
  - Design with Focus on Development
  - Mainly from regulation instances

Context: User-Flows in App Stores



The Problem: F-Droid*

- → **Discrepancy by F-Droid users**

  - Few well-informed privacy advocats

- → **Anti-Features**

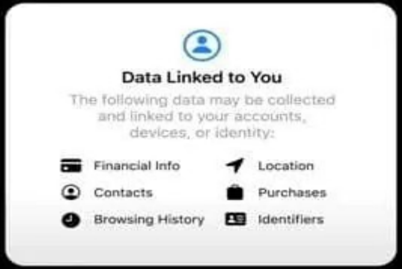
  - Incomprehensible to the common users

- → **Exodus Privacy**

  - Privacy-related open-database of Android apps

* F-Droid is the main distribution mean for free open-source software ("FOSS") for Android devices and main Play Store alternative

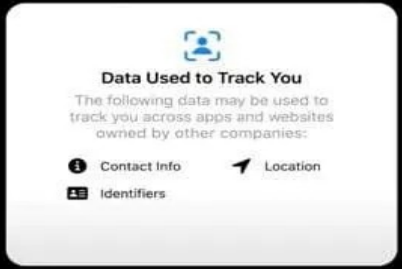
Inspiration: Privacy Visualization Designs



Data Linked to You

The following data may be collected and linked to your accounts, devices, or identity:

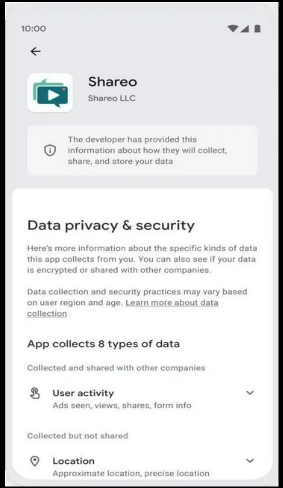
Financial Info
Location
Contacts
Purchases
Browsing History
Identifiers



Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

Contact Info
Location
Identifiers



Shareo
Shareo LLC

The developer has provided this information about how they will collect, share, and store your data

Data privacy & security

Here's more information about the specific kinds of data this app collects from you. You can also see if your data is encrypted or shared with other companies.

Data collection and security practices may vary based on user region and age. Learn more about data collection

App collects 8 types of data

Collected and shared with other companies

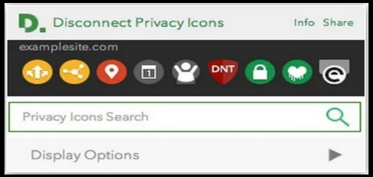
User activity
Ads seen, views, shares, form info

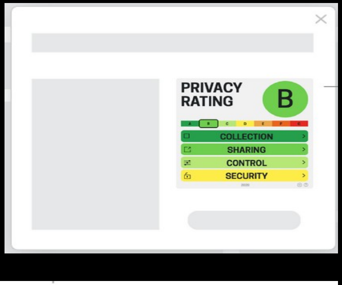
Collected but not shared

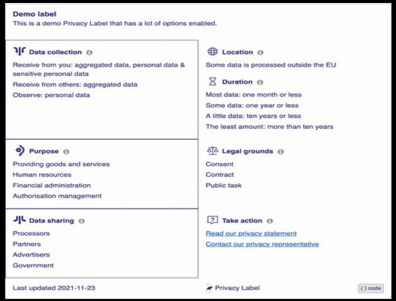
Location
Approximate location, precise location

Digital Gatekeeper

Literature







Demo label
This is a demo Privacy Label that has a lot of options enabled.

Data collection
Receive from you: aggregated data, personal data & sensitive personal data
Receive from others: aggregated data
Observe: personal data

Location
Some data is processed outside the EU

Duration
Most data: one month or less
Some data: one year or less
A little data: ten years or less
The least amount: more than ten years

Purpose
Providing goods and services
Human resources
Financial administration
Authorisation management

Legal grounds
Consent
Contract
Public task

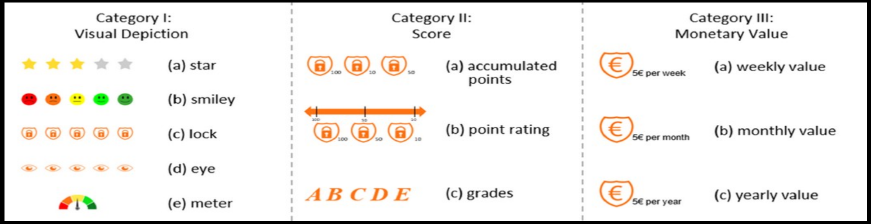
Data sharing
Processors
Partners
Advertisers
Government

Take action
Read our privacy statement
Contact our privacy representative

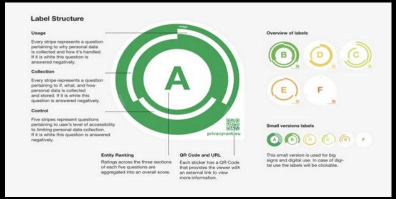
Last updated 2021-11-23

Privacy Label

{ } code



Category I: Visual Depiction	Category II: Score	Category III: Monetary Value
(a) star	(a) accumulated points	(a) weekly value
(b) smiley	(b) point rating	(b) monthly value
(c) lock	(c) grades	(c) yearly value
(d) eye		
(e) meter		



Label Structure

Usage
Every stripe represents a question pertaining to why personal data is collected and how it's handled. If it is white this question is answered negatively.

Collection
Every stripe represents a question pertaining to if, what, and how personal data is collected and stored. If it is white this question is answered negatively.

Control
Five stripes represent questions pertaining to user's level of accessibility to limiting personal data collection. If it is white this question is answered negatively.

Entity Ranking
Ratings across the three sections of each five questions are aggregated into an overall score.

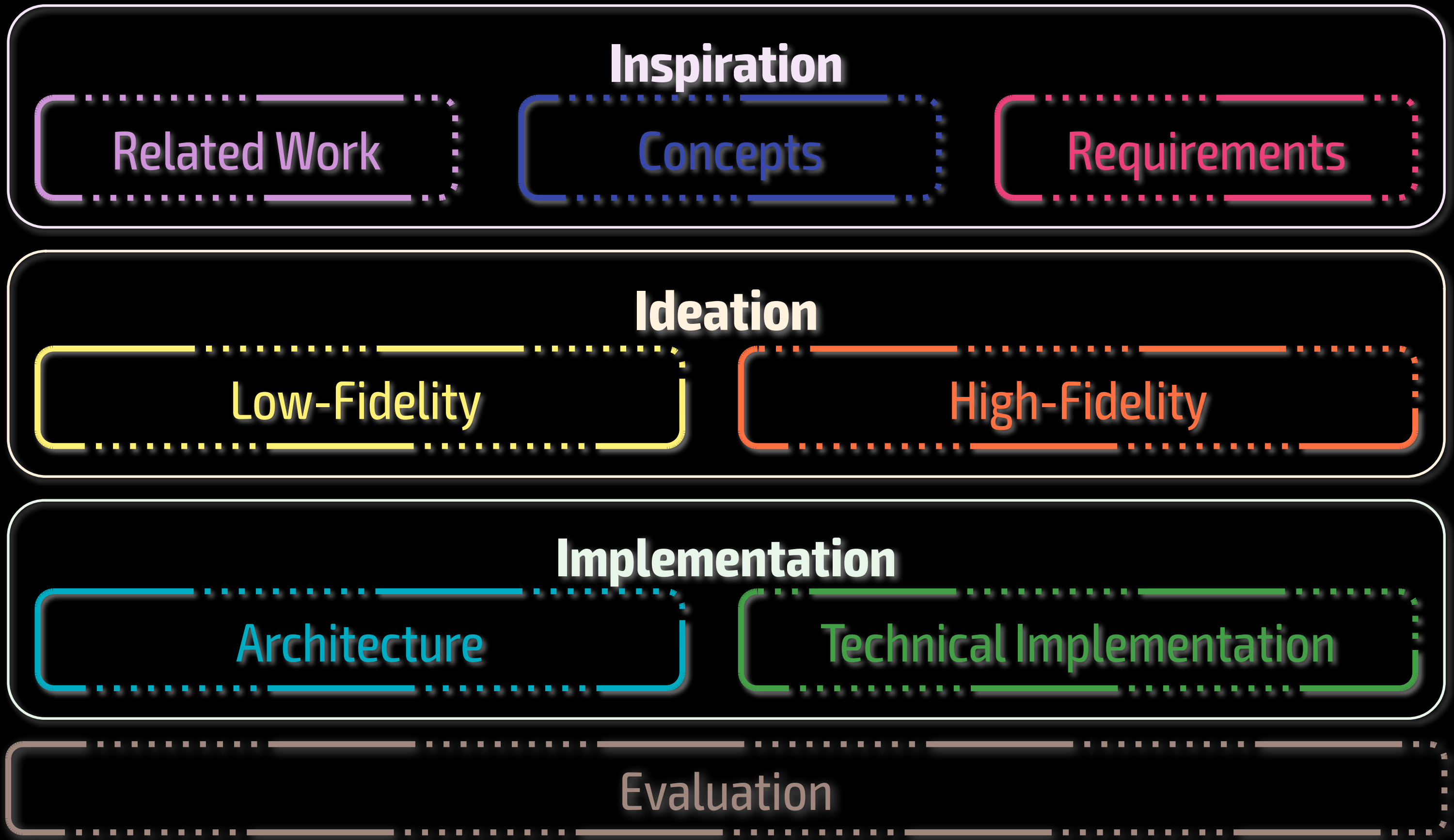
QR Code and URL
Each sticker has a QR Code that provides the viewer with an external link to view more information.

Overview of labels

Small versions labels

This small version is used for big signs and digital use. In case of digital use the labels will be clickable.

Procedure



Inspiration

Related Work

Concepts

Requirements

Ideation

Low-Fidelity

High-Fidelity

Implementation

Architecture

Technical Implementation

Evaluation

Motivation & Research Questions

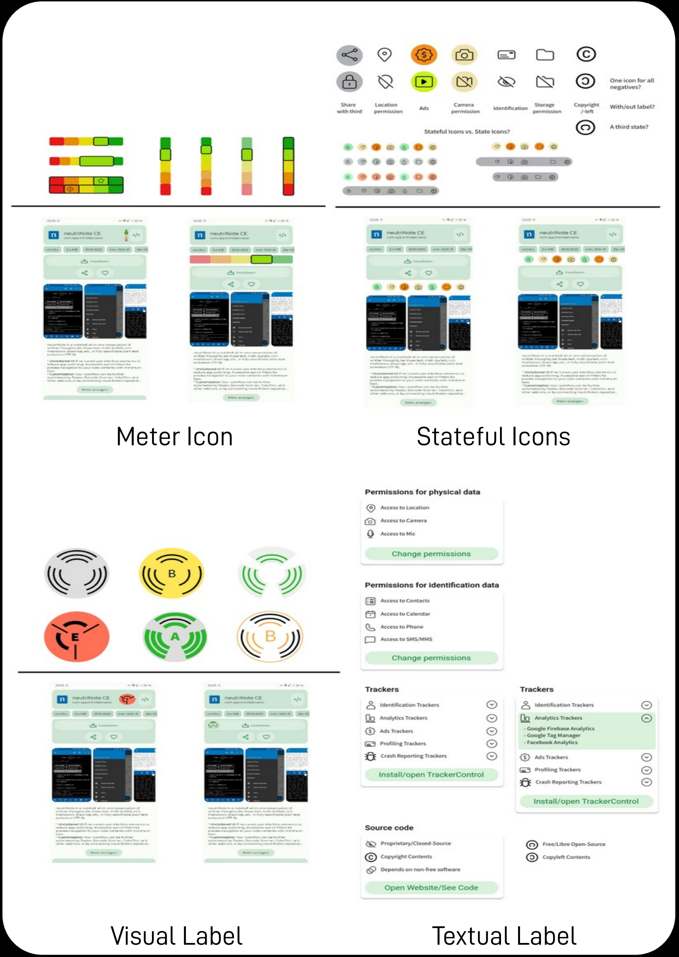
- F-Droid lacking intuitive tool to empower users making informed decisions concerning privacy
- Privacy visualizations in the literature have not been tested with users at all and lacking an interactive-interface
- Me being the developer of Neo Store, an F-Droid client

? *What privacy visualization designs already exist and what are the advantages of one over the other?*

? *Which of the identified privacy visualization systems would the project's community prefer, and what improvements could be made?*

Ideation

- Low Fidelity
  - Sketching
    - Based on literature designs
  - Expert Interviews
    - Semi-structured: Qualitative, Subjective & Efficient
- High-Fidelity
  - Integrate Feedback & Iterate
    - Design Decisions
  - Complementing the Concept
    - Defining a Framework



Meter Icon

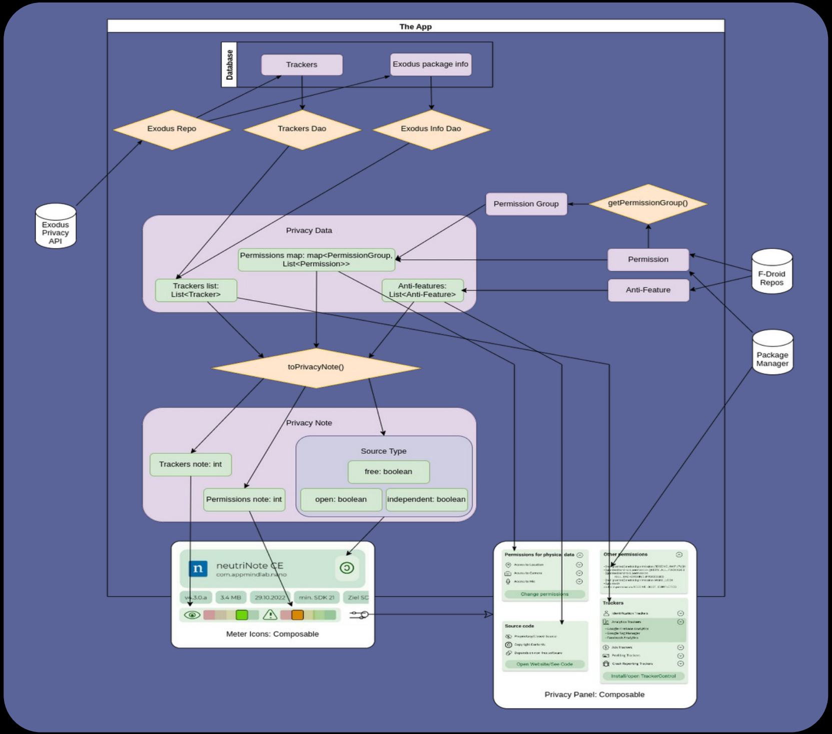
Stateful Icons

Visual Label

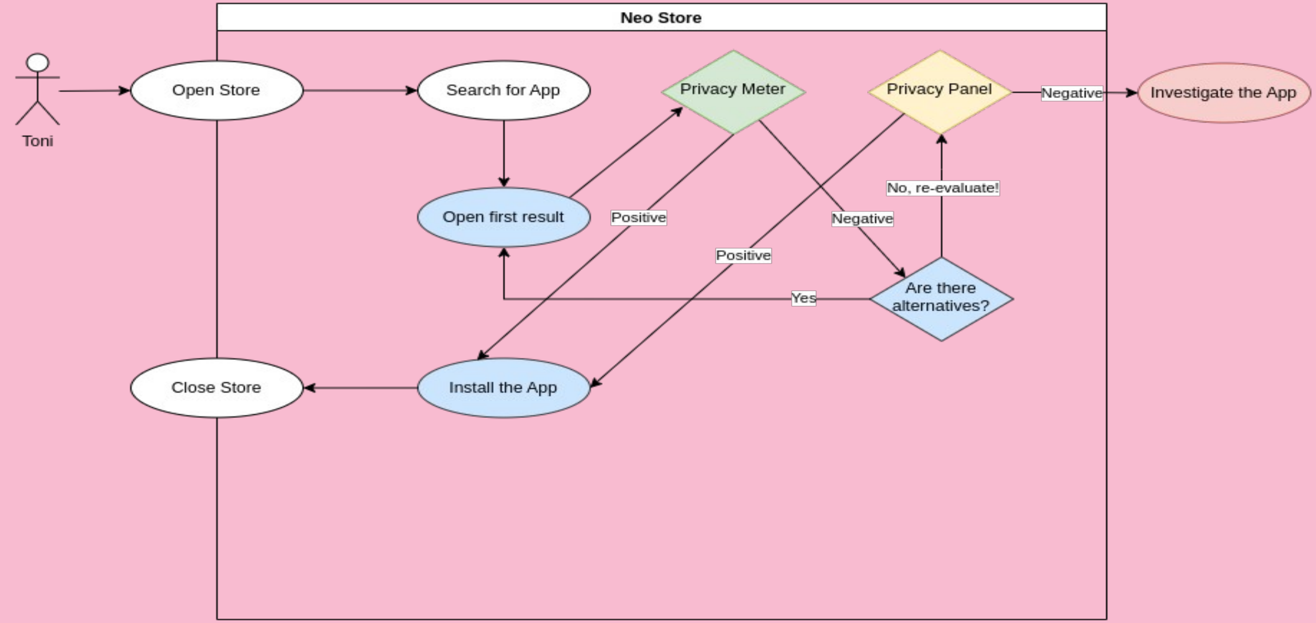
Textual Label

Implementation

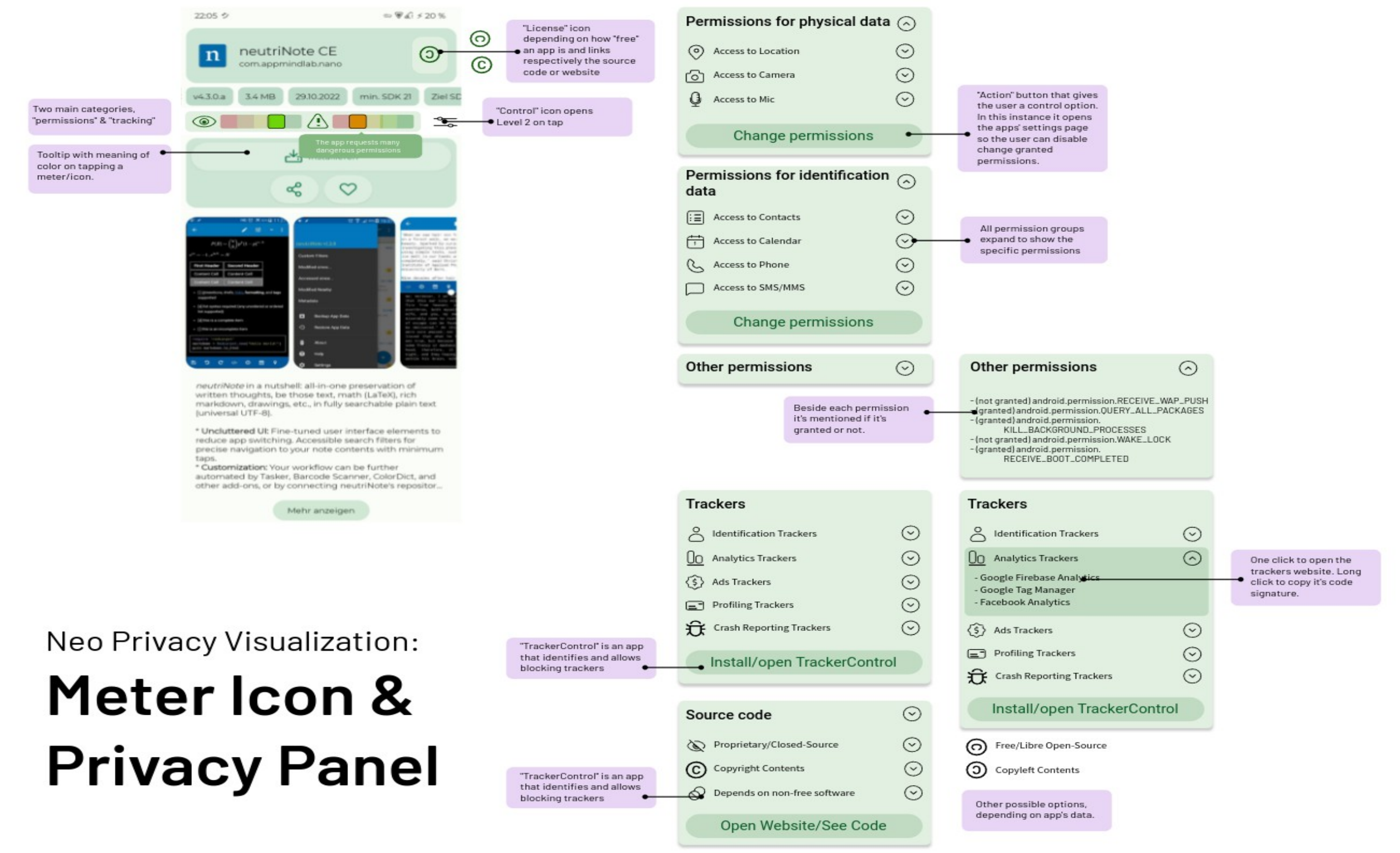
- Architecture
  - Specifying Objects Data
  - Mapping Data Structure to Layout
- Technical Implementation
  1. Backend
  2. Privacy Processor
  3. Frontend



Result: User-Flow



Result: Neo Privacy Visualization Design



22:05 · 20 %

neutriNote CE
com.appmindlab.nano

v4.3.0.a · 3.4 MB · 29.10.2022 · min. SDK 21 · Ziel SD

"License" icon depending on how "free" an app is and links respectively the source code or website

Two main categories, "permissions" & "tracking"

"Control" icon opens Level 2 on tap

The app requests many dangerous permissions

Tooltip with meaning of color on tapping a meter/icon.

neutriNote in a nutshell: all-in-one preservation of written thoughts, be those text, math (LaTeX), rich markdown, drawings, etc., in fully searchable plain text (universal UTF-8).

* **Uncluttered UI:** Fine-tuned user interface elements to reduce app switching. Accessible search filters for precise navigation to your note contents with minimum taps.
* **Customization:** Your workflow can be further automated by Tasker, Barcode Scanner, ColorDict, and other add-ons, or by connecting neutriNote's repositor...

Mehr anzeigen

Permissions for physical data

- Access to Location
- Access to Camera
- Access to Mic

Change permissions

"Action" button that gives the user a control option. In this instance it opens the apps' settings page so the user can disable change granted permissions.

Permissions for identification data

- Access to Contacts
- Access to Calendar
- Access to Phone
- Access to SMS/MMS

Change permissions

All permission groups expand to show the specific permissions

Other permissions

Beside each permission it's mentioned if it's granted or not.

Other permissions

- (not granted) android.permission.RECEIVE_WAP_PUSH
- (granted) android.permission.QUERY_ALL_PACKAGES
- (granted) android.permission.
KILL_BACKGROUND_PROCESSES
- (not granted) android.permission.WAKE_LOCK
- (granted) android.permission.
RECEIVE_BOOT_COMPLETED

Trackers

- Identification Trackers
- Analytics Trackers
- Ads Trackers
- Profiling Trackers
- Crash Reporting Trackers

Install/open TrackerControl

"TrackerControl" is an app that identifies and allows blocking trackers

Trackers

- Identification Trackers
- Analytics Trackers
  - Google Firebase Analytics
  - Google Tag Manager
  - Facebook Analytics
- Ads Trackers
- Profiling Trackers
- Crash Reporting Trackers

Install/open TrackerControl

One click to open the trackers website. Long click to copy it's code signature.

Neo Privacy Visualization:

Meter Icon & Privacy Panel

Source code

- Proprietary/Closed-Source
- Copyright Contents
- Depends on non-free software

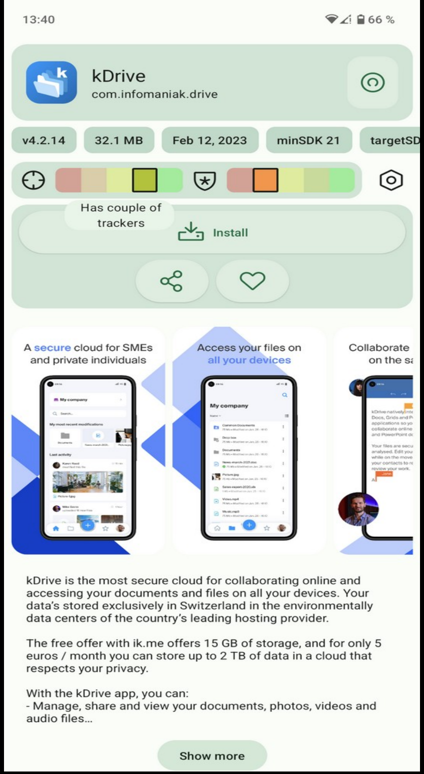
Open Website/See Code

"TrackerControl" is an app that identifies and allows blocking trackers

- Free/Libre Open-Source
- Copyleft Contents

Other possible options, depending on app's data.

Result: Neo Privacy Visualization



13:40 66 %

kDrive
com.infomaniak.drive

v4.2.14 | 32.1 MB | Feb 12, 2023 | minSDK 21 | targetSD

Has couple of trackers

Install

A secure cloud for SMEs and private individuals

Access your files on all your devices

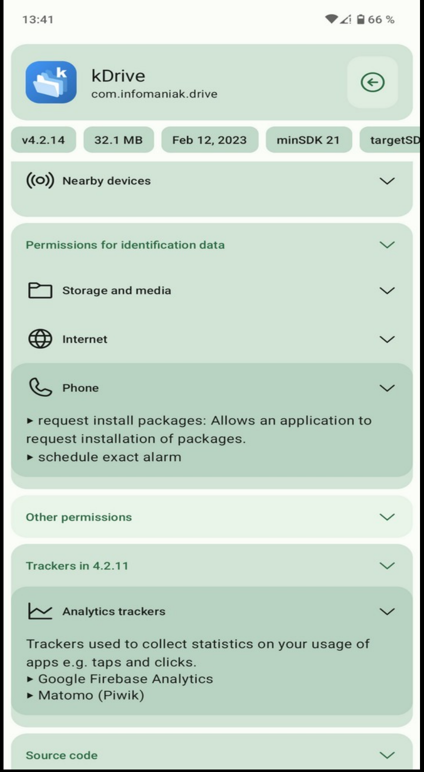
Collaborate on the s

kDrive is the most secure cloud for collaborating online and accessing your documents and files on all your devices. Your data's stored exclusively in Switzerland in the environmentally data centers of the country's leading hosting provider.

The free offer with ik.me offers 15 GB of storage, and for only 5 euros / month you can store up to 2 TB of data in a cloud that respects your privacy.

With the kDrive app, you can:
- Manage, share and view your documents, photos, videos and audio files...

Show more



13:41 66 %

kDrive
com.infomaniak.drive

v4.2.14 | 32.1 MB | Feb 12, 2023 | minSDK 21 | targetSD

Nearby devices

Permissions for identification data

Storage and media

Internet

Phone

- request install packages: Allows an application to request installation of packages.
- schedule exact alarm

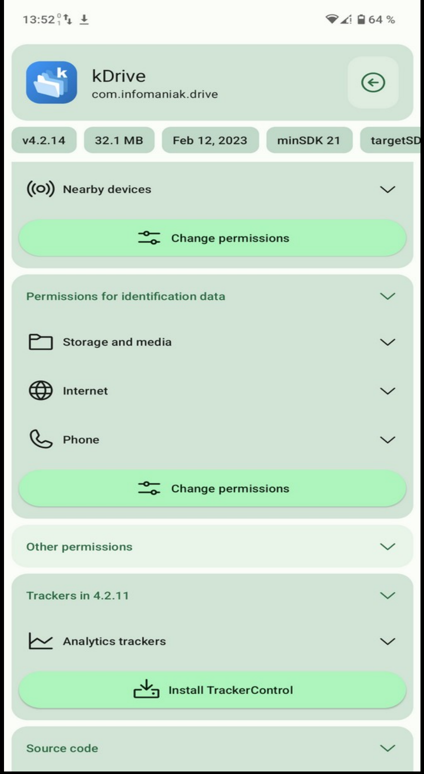
Other permissions

Trackers in 4.2.11

Analytics trackers

Trackers used to collect statistics on your usage of apps e.g. taps and clicks.
- Google Firebase Analytics
- Matomo (Piwik)

Source code



13:52 64 %

kDrive
com.infomaniak.drive

v4.2.14 | 32.1 MB | Feb 12, 2023 | minSDK 21 | targetSD

Nearby devices

Change permissions

Permissions for identification data

Storage and media

Internet

Phone

Change permissions

Other permissions

Trackers in 4.2.11

Analytics trackers

Install TrackerControl

Source code

Result: Evaluation

Open-survey on interpretation and preferences. 16 participants & self-assessment of privacy awareness, privacy considerations and IT background

- Privacy Meter Icon rightly interpreted
- Design preferences?
  - "First of all: visual [l]abel is horrible to understand…"
  - Meter Icon 9-7 Stateful Icons: Similar preferences and arguments as the experts, mostly centered around simplicity and intuitiveness
- Expectation considering the gateway icon kinda right (9/16)
- Privacy Panel was welcomed by most users (13/16)

Insights

- ♦ Intuitiveness is the Queen/King
  - ➔ The decisive factor for most users
- ♦ Multi-layered Visualizations
  - ➔ Covering Simplicity & Informativeness
- ♦ Differentiate Privacy Visualization
  - ➔ Design preferences differ based on user's privacy awareness

Future Work

- Privacy by Design Guidelines
  - ➔ On its way!
- Contextualization of Permissions
  - ➔ AI-Modell?
- Server-side implementation
  - ➔ In F-Droid's meta-data?

Context: Privacy & Software

- **Privacy Visualizations**
  - User-facing aspect
  - Design with Focus on UX
  - Mainly from UX researches

- **Privacy by Design Guidelines**
  - Developer-facing aspect
  - Design with Focus on Development
  - Mainly from regulation instances

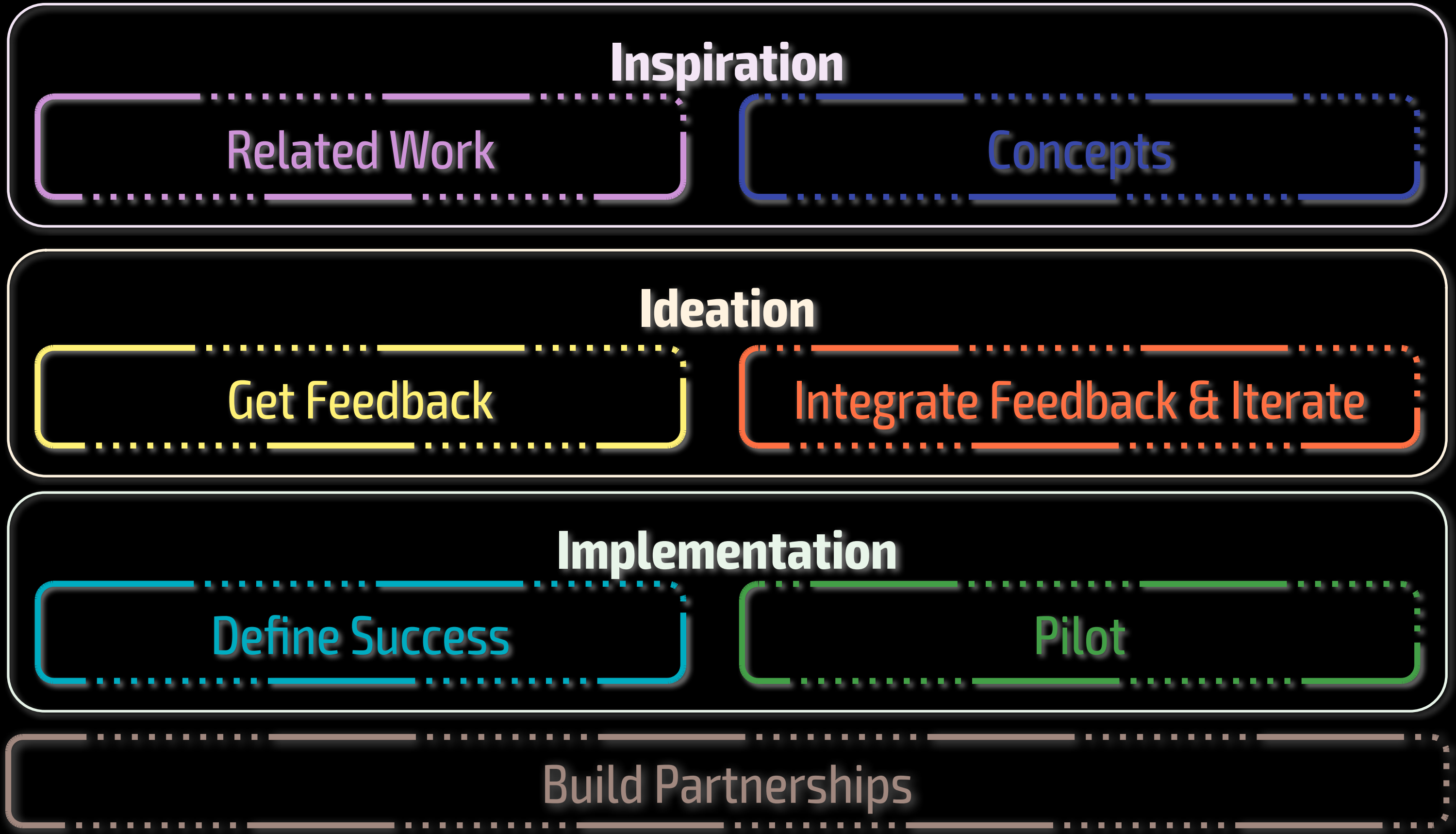
Motivation & Research Questions

- Most PbD guidelines being enforced by regulatory instances
- Giving voice for FOSS developers on the development of such guidelines
- Modeling of PbD guidelines for open source developers

? *What PbD guidelines already exist, and what are the advantages of some over others for the FOSS community?*

? *What aspects of the identified PbD guidelines make sense from the perspective of the open source community and developer, and what could be improved?*

Procedure



Inspiration

Related Work

Concepts

Ideation

Get Feedback

Integrate Feedback & Iterate

Implementation

Define Success

Pilot

Build Partnerships

Ideation & Implementation

- Ideation

  - Expert Interviews: Privacy Rights & PbD Principles

  - Prototype: PbD Principles

- Implementation

  - Community-survey: PbD Principles

  - PbD Guidelines: Publication

Ideation Result: Privacy Rights

Rights	
For Individuals to Exercise Their Rights	To Object Marketing
To Be Informed	To Object Automated Decision-Making
Individuals Access	Withdraw Consent
Rectification	Complain
Erasure	For Individuals Not to Be Discriminated (based on their choices)
Restriction of Processing	**Choice:** Data as enforced excess turnover for companies, over the payment (e.g. in games).
Data Portability	**Anti-discrimination:** respecting the rights of minorities.
To Object	**Awareness:** educating users on their rights explicitly.

Ideation Result: PbD Principles

Principles	
Transparency (4/6)	**Right to be forgotten (2/6)**
Purpose Limitation (2/6)	Adoption, Use or Disclosure of an identifier
Limiting Use and Disclosure (1/6)	Cross-border Transfer
Data Minimization (3/6)	Lawfullness
Correctness	Disclosure
Retention	Sale
Security (1/6)	Share
Accountability	Dealing with Unsolicited Personal Data
Anonymity and Pseudonymity	Source
Consent (5/6)	**Assistance for Users**
Control (3/6)	**Data Loss Precautions**
Functionality	**Education**

Ideation Result: Highlights

Principle	Comments
Cross-border Transfer	“I'm living in [a non-free country] and would prefer to transfer my data to other countries.” “From european perspective it's much important. China is more critical. USA is kinda less critical as some social initiatives provide their services from their.”
Adoption, Use or Disclosure of an identifier	“Using codes/keys that aren't linked to the full data may be helpful.”
Share	“Collecting data only with consent and data should be also open [access].”
Retention	“Rubber paragraph, Automatic deletion is conflicting (opt-in vs opt-out).”
Security	“Most security features [come] from […] infrastrcture and libraries [we use], this is a technical problem”
Accountability	“Privacy of developers should also be protected e.g. GPL also says we have no responsibility”
Disclosure (to law enforcement)	“Very controversial! If legit or no is too complex.”
Assistance for Users	Building community as a solution
Data Loss Precautions	As users' data is mainly theirs!
Education	“average users may not understand how they may profit from privacy”

Current Insights

- ♦ All privacy rights make sense
  - ➔ Can also be sharpened to clear up misunderstandings
- ♦ Overlapping of many principles
  - ➔ Simplify with precise set of essential principles
- ♦ FOSS developers are under-resourced
  - ➔ Renders some principles or even legal requirements unrealistic

Ideation & Implementation

→ Ideation

- Expert Interviews: Privacy Rights & PbD Principles
- Prototype: PbD Principles

→ Implementation

- Community-survey: PbD Principles 10/1 - 10/16
- PbD Guidelines: Publication 11/01

→ Building Partnerschips

- Open discussion with the FOSS community on the guidelines (e.g. in Workshops)

Issues

- **Social**: Diversity among the community
- **Security**: Reluctance of some community members
- **Scope**: Being limited by thesis scope (e.g. extending work to Nudges vs. Boosts) or reach (e.g. mostly Android community)

✗ Documentation

✗ Related Links

✗ Updates

Thanks for keeping up!
Any Questions?