UCLouvain

Building private-by-design IoT systems

Igor Zavalyshyn post-doc @UCLouvain

CyberExcellence Seminar, May 23rd 2022

Context

- Internet of Home Things aka Smart Home
- PhD results and post-doc followup

  + general trends and observations
- High-level overview

Internet of home things

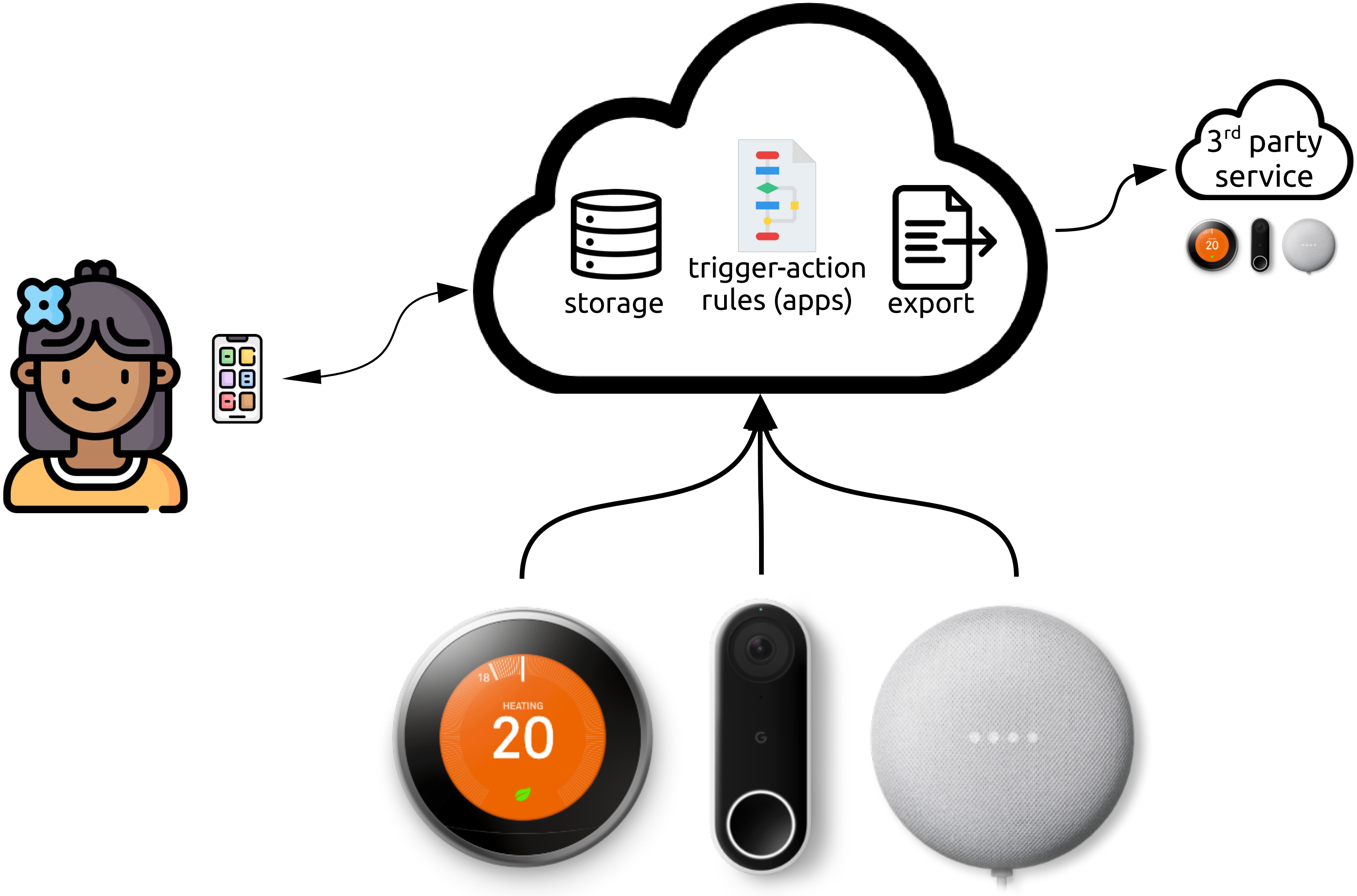
Internet of spying things

Control

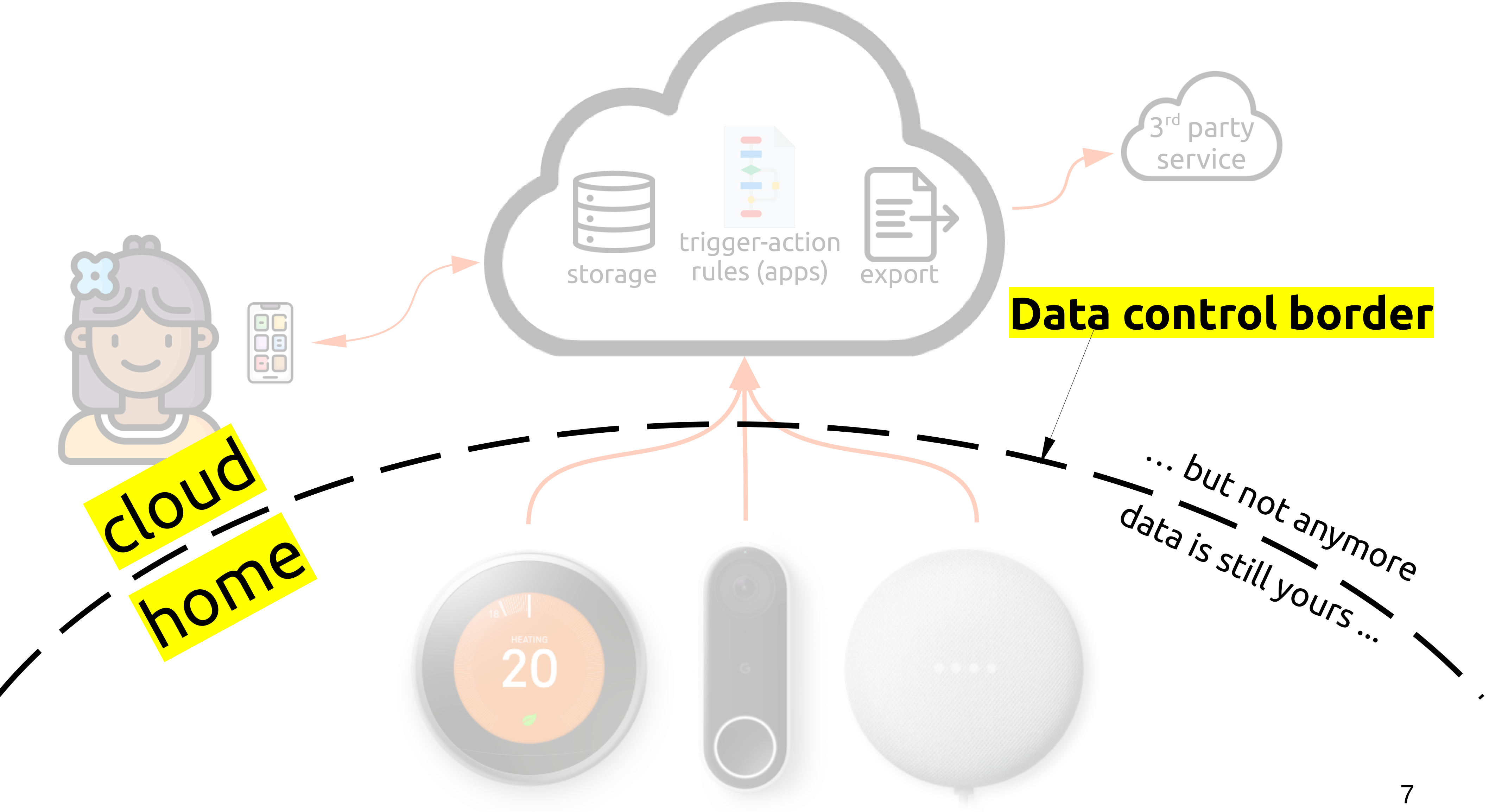
Watch

Listen

How does it usually work?



How does it usually work?



storage

trigger-action rules (apps)

export

3rd party service

Data control border

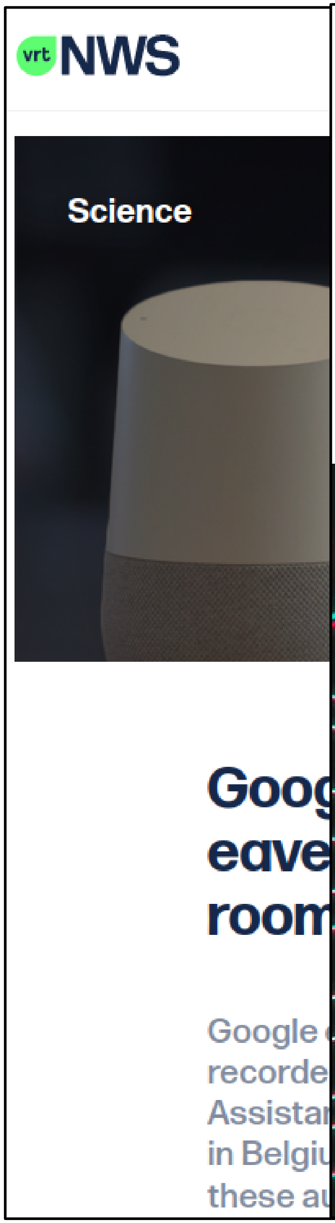
cloud

home

... but not anymore

data is still yours ...

Why do you care?

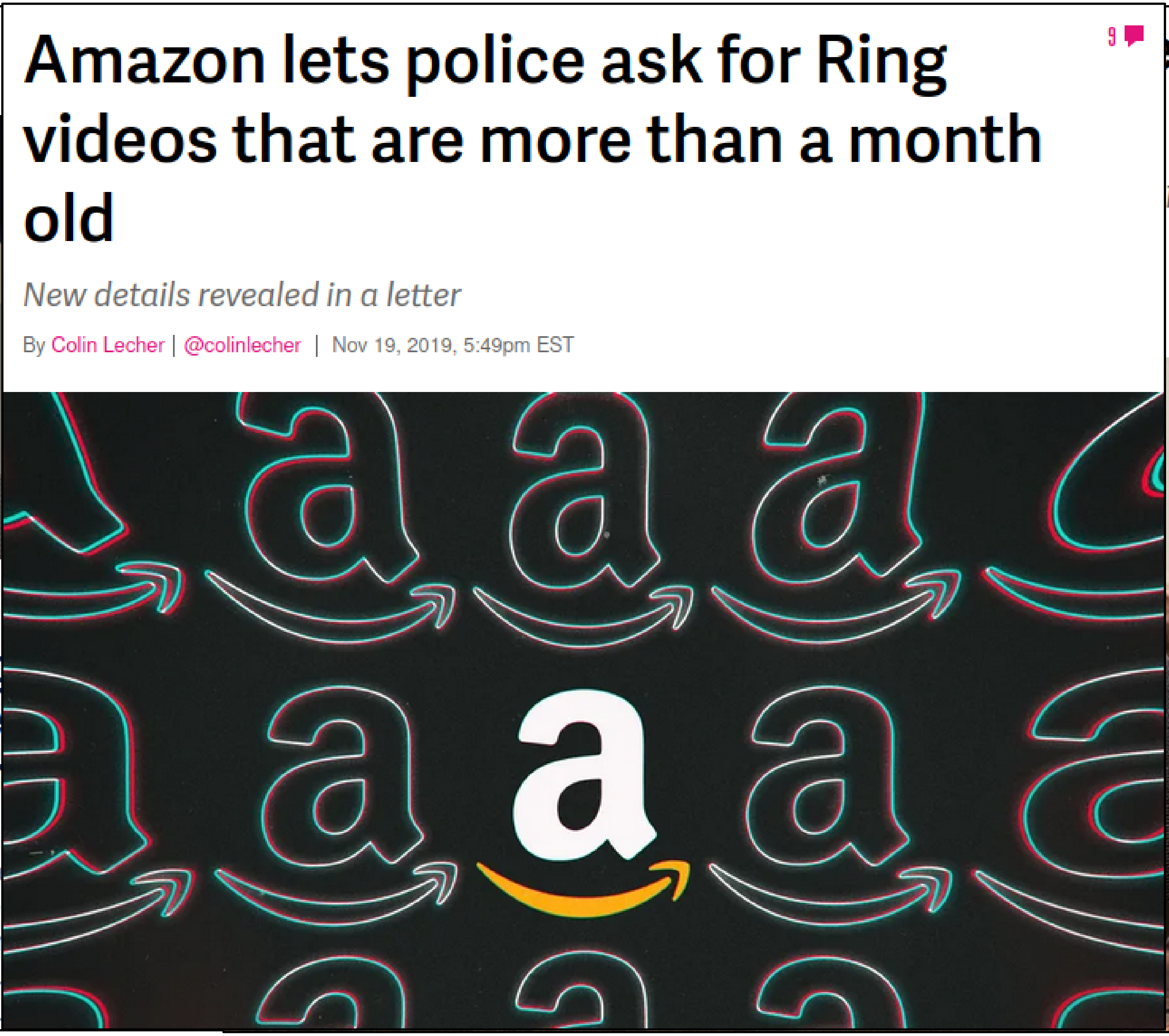


vrt NWS

Science

Goog
eave
room

Google
recorde
Assista
in Belgiu
these au

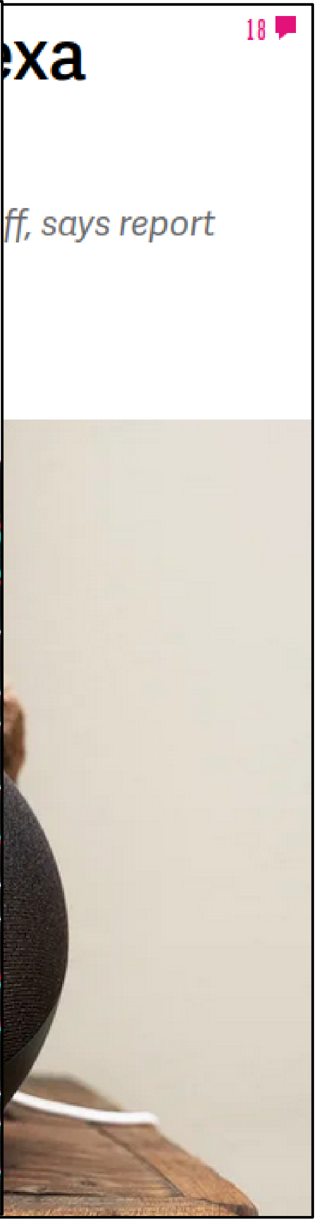


9

Amazon lets police ask for Ring videos that are more than a month old

New details revealed in a letter

By Colin Lecher | @colinlecher | Nov 19, 2019, 5:49pm EST



18

exa

ff, says report

so, what can we do?

keep it all local

secure it in the cloud

offer users a choice

so, what can we do?

keep it
all local

HomePad
SEC’18

secure it in
the cloud

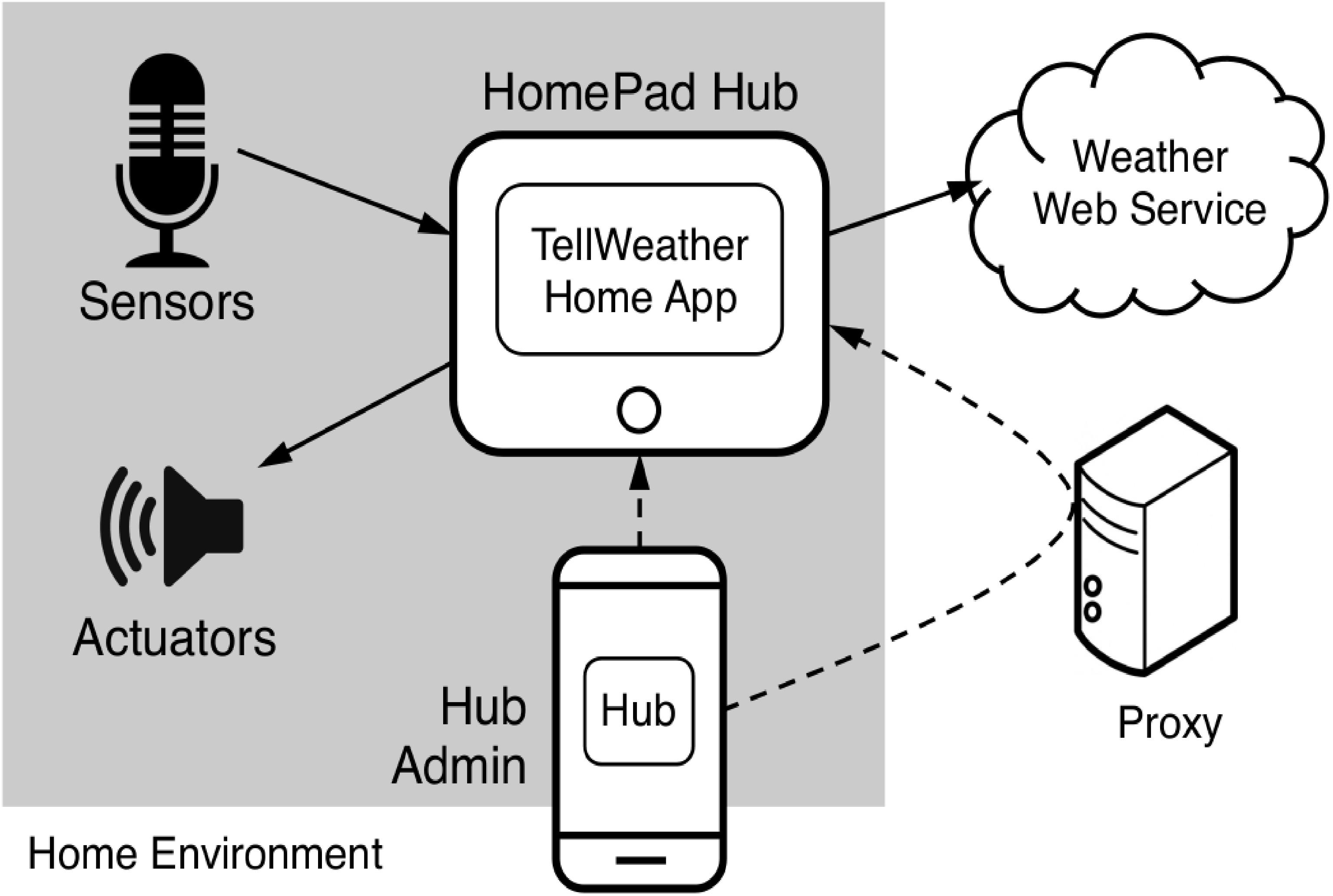
PatrIoT
Mobiquitous’20

offer users
a choice

SoK
PETS’22

HomePad

Personal smart hub



HomePad features

local-first data processing

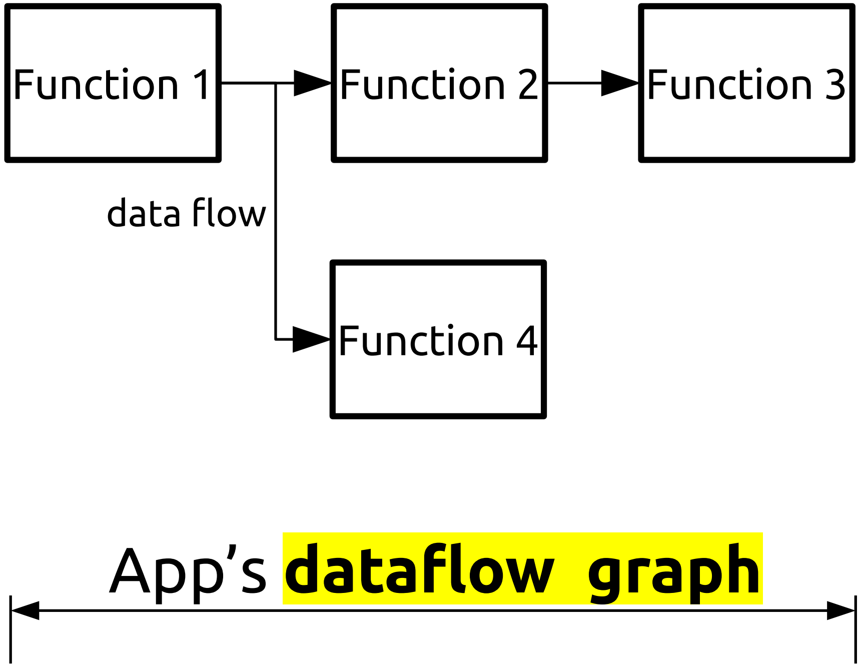
dataflow-based programming

rich set of built-in API functions

drivers for smart home devices

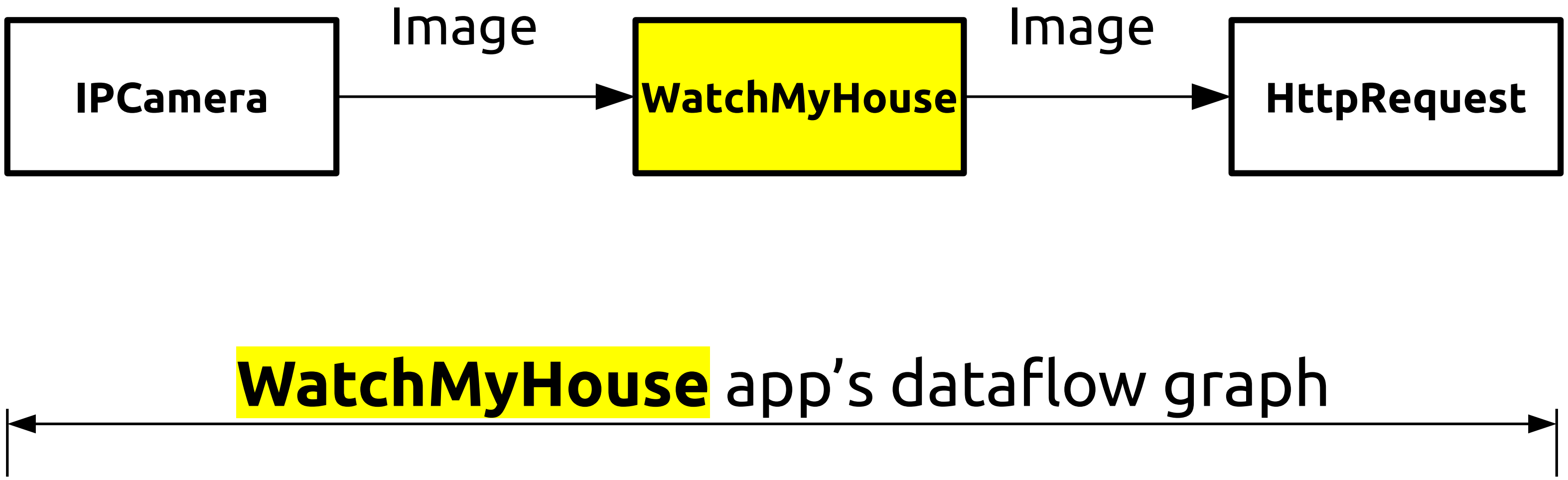
Dataflow programming

old style app (monolith)

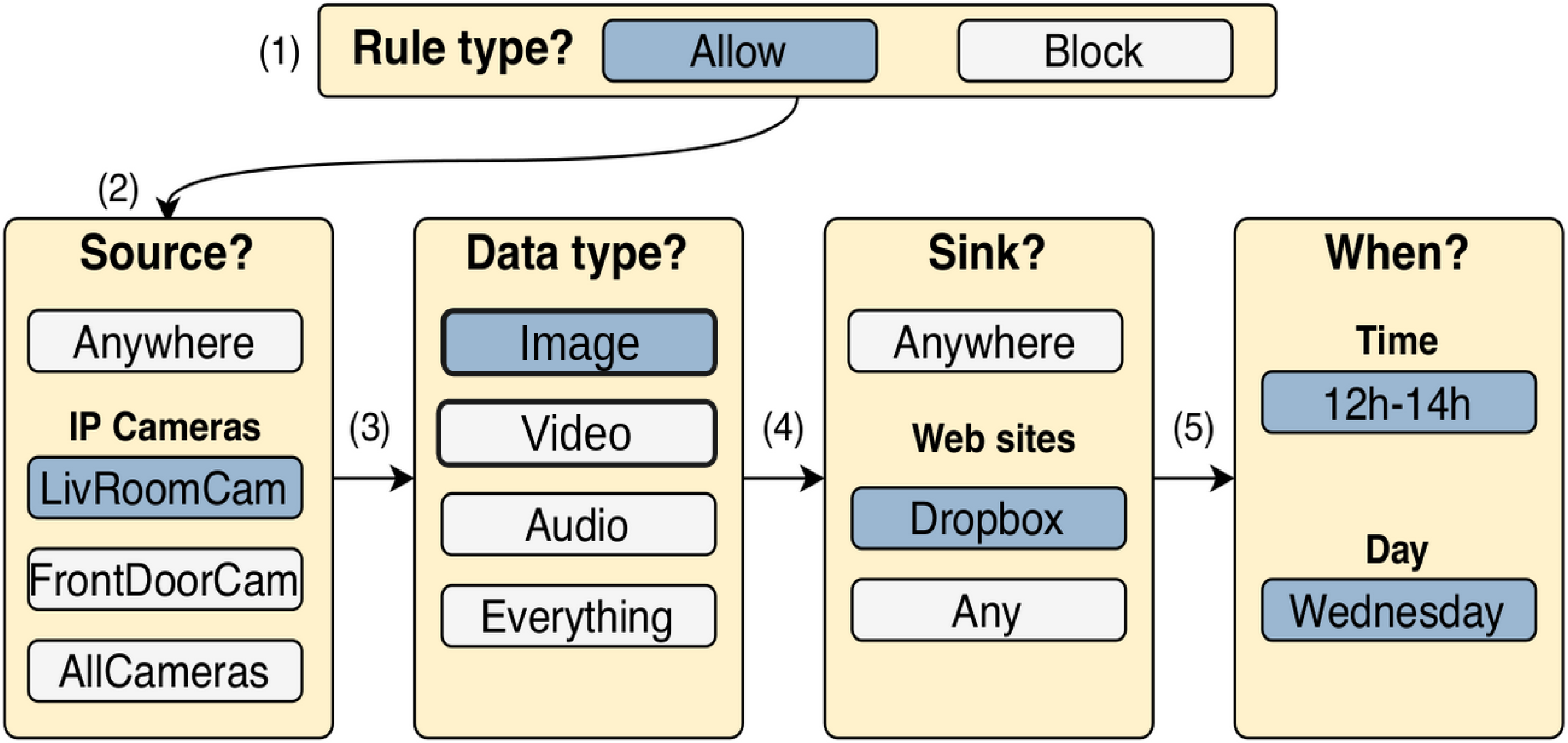


App's **dataflow graph**

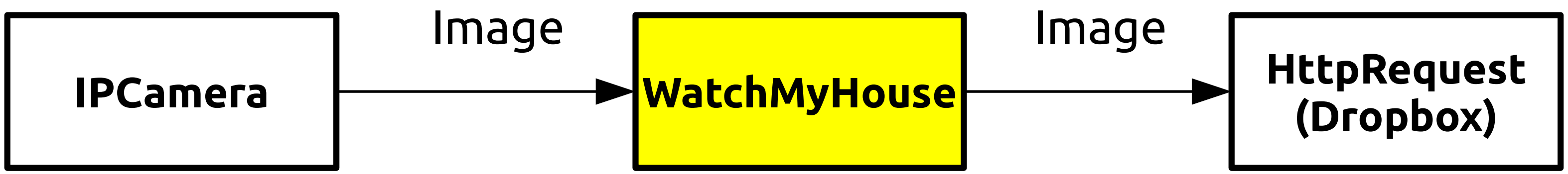
Dataflow programming



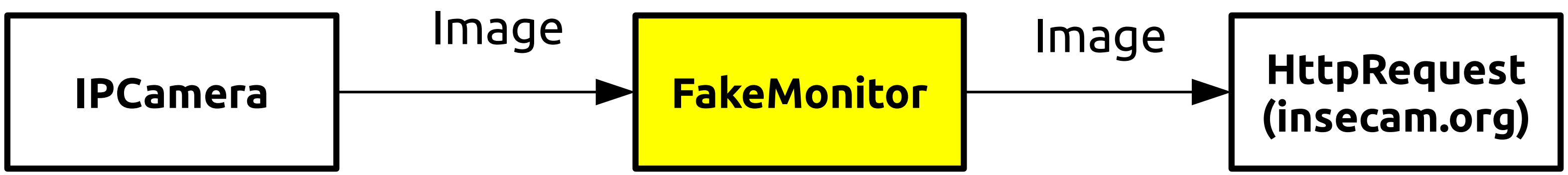
Privacy policy UI



Flows tracking & control

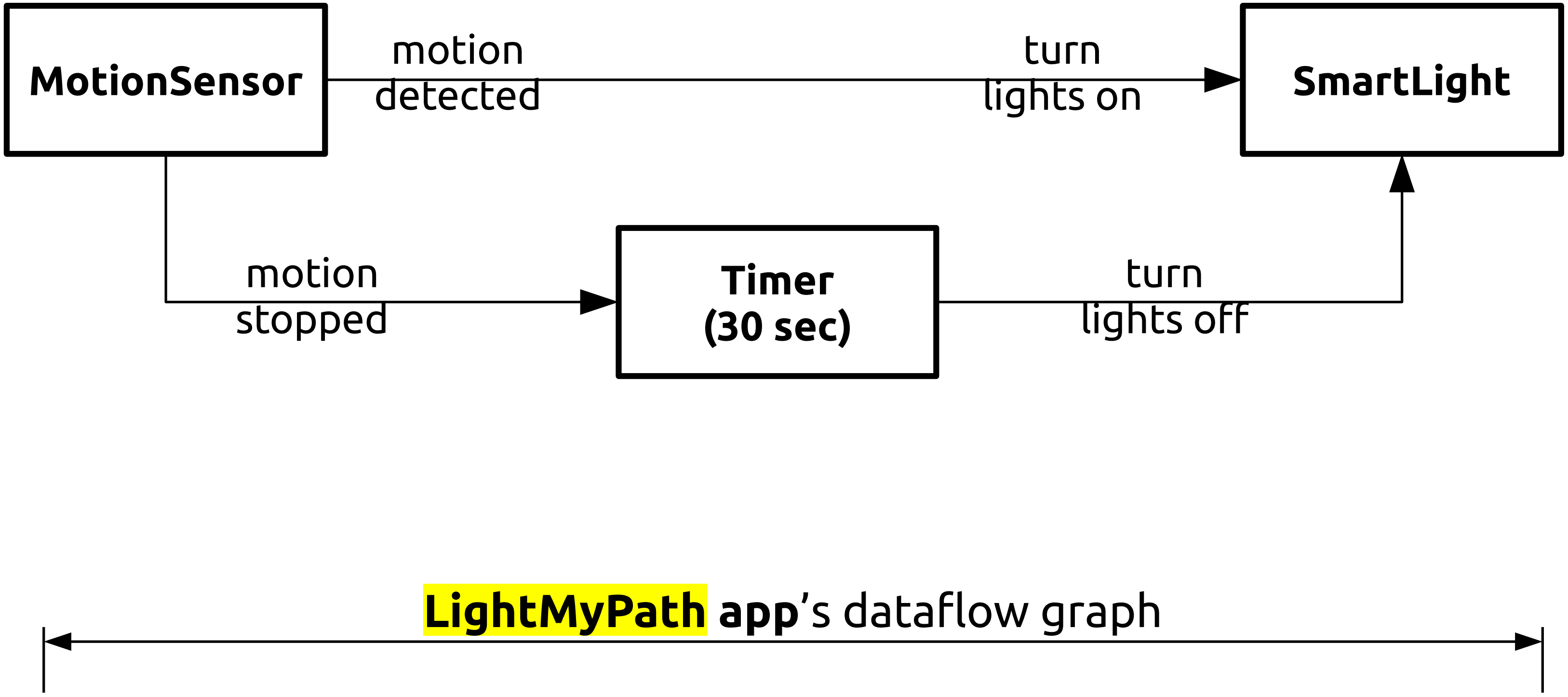


Source:	**Datatype:**	**Sink:**	**Action:**
LivRoomCam	Image	Dropbox	Allow Wed, 12-14



Source:	**Datatype:**	**Sink:**	**Action:**
LivRoomCam	Image	insecam.org	Block

No-code apps



LightMyPath app's dataflow graph

Summary

local-first data processing
local privacy control
shortcomings:
- access to the cloud resources
- lack of computing/storage

PatrIoT

Meet PatrIoT

platform provider ≠ data owner & processor

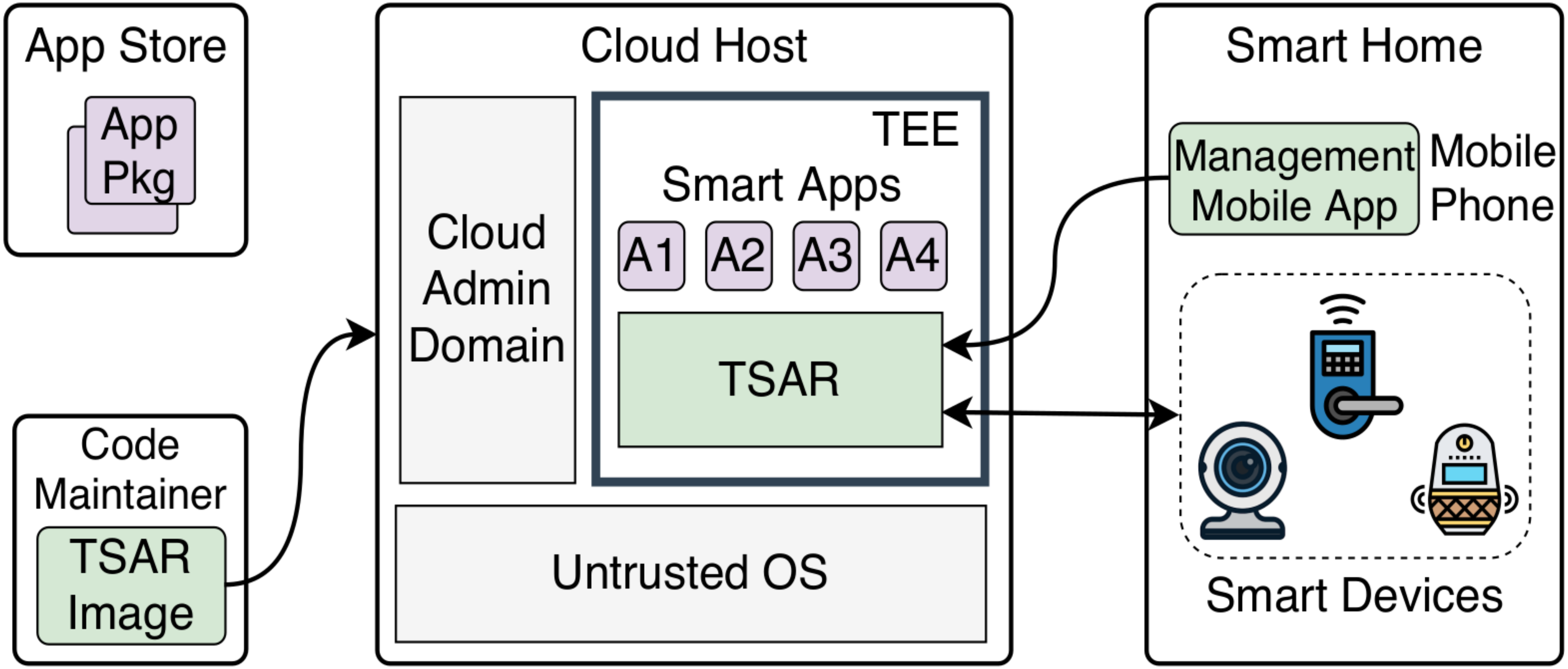
extends dataflow model to the cloud

secure (SGX) and private by design

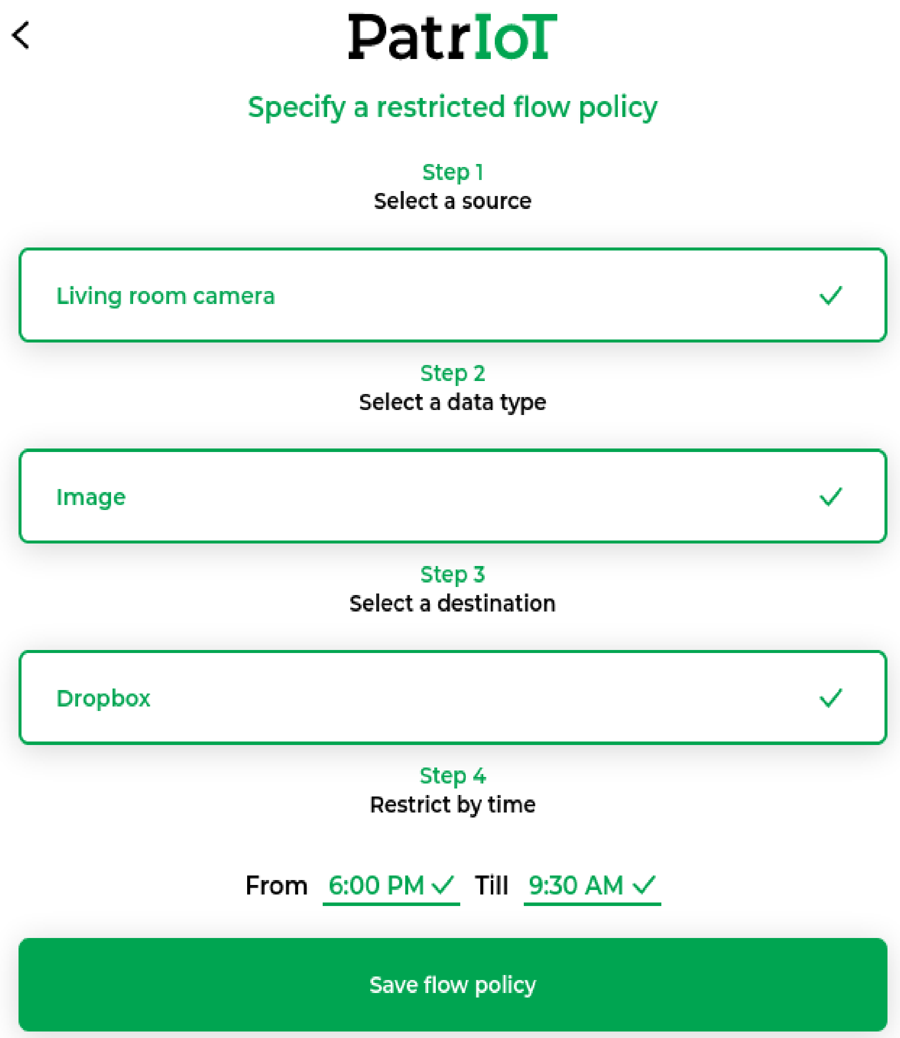
self-hosted or provided as a service

offers full control to the user

PatrIoT system model



PatrIoT UI



PatrIoT

Specify a restricted flow policy

Step 1
Select a source

Living room camera ✓

Step 2
Select a data type

Image ✓

Step 3
Select a destination

Dropbox ✓

Step 4
Restrict by time

From 6:00 PM ✓ Till 9:30 AM ✓

Follows the

data source

data type

data sink

+ context

model

Summary

personal smart home platform
secure and verifiable
shortcomings
  it’s a clean-slate design
  existing services need to adopt/adapt

Next generation smart home systems

Goals

Find an alternative to local-only and cloud-only

Require minimal changes to existing infrastructure and workflow

Offer users a way to decide on a privacy-vs-utility trade off

Research

- Analysis of existing smart home systems *"SoK: Privacy-enhancing Smart Home Hubs", PETS'22*
- 10 commercial & open source systems + 37 papers
- **What was analyzed?**
  - System and threat models
  - Stakeholders share, place of activity
  - Implemented PET types

Insights

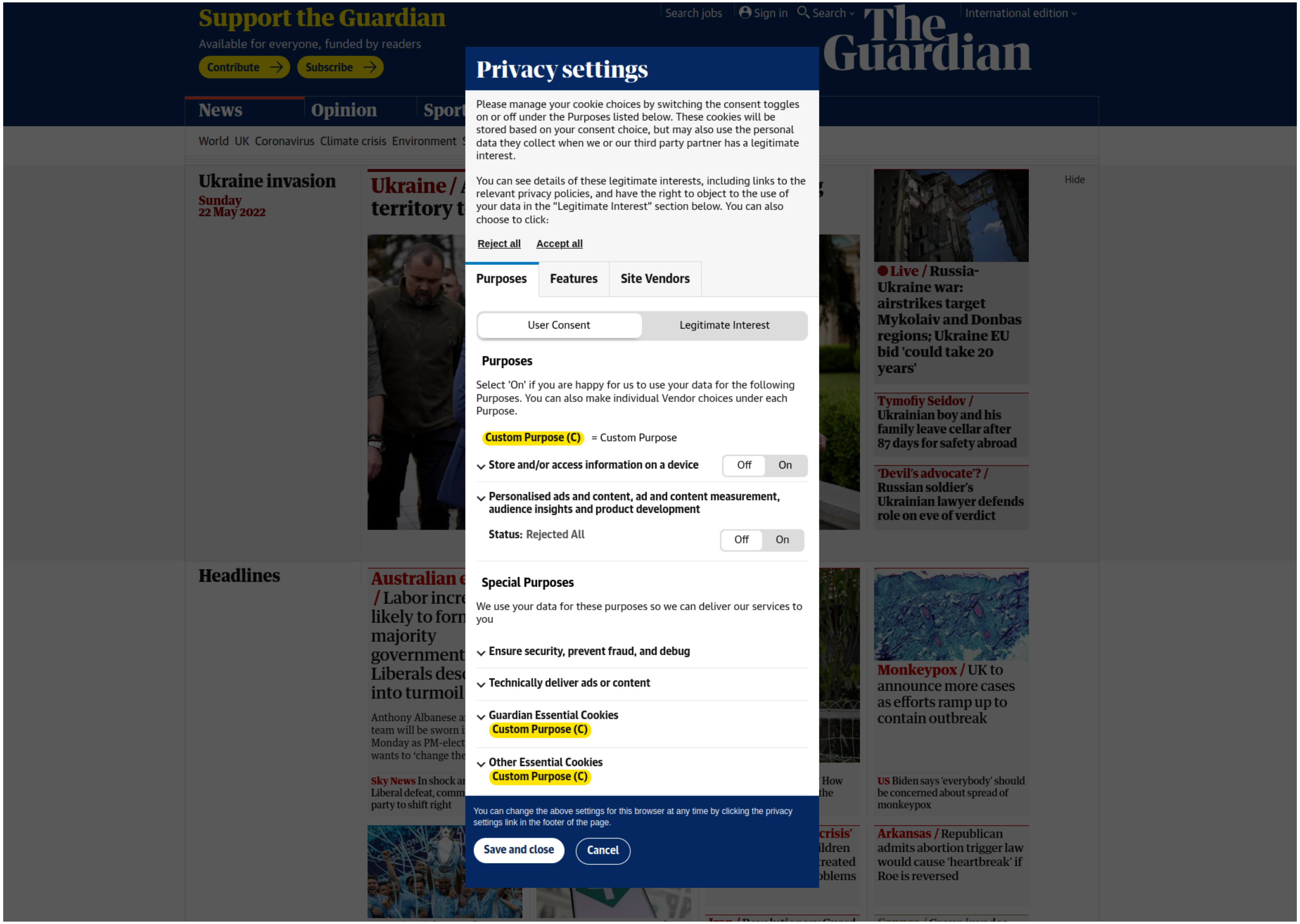
- Alarming trend: commercial systems often monopolize devices, apps and cloud servers.
- Commercial systems are increasingly cloud dependent, open source ones run locally.
- Lack of privacy control vs. lack of functionality
- A promising shift towards hub-first or hybrid design among a few commercial systems.
- But threats associated with platform provider are mostly neglected.

More Insights (academic)

- Proprietary device software and protocols make privacy control harder.
- Hybrid designs are often proposed but require significant changes in existing systems design.
- Lack of suitable system support for hybrid design of smart home services:
  - deployment, resource provisioning, access control, privacy enforcement ...

HubOS

Remember cookies?



Ukraine invasion
Sunday 22 May 2022

Ukraine / … territory t…

● Live / Russia-Ukraine war: airstrikes target Mykolaiv and Donbas regions; Ukraine EU bid 'could take 20 years'

Tymofiy Seidov / Ukrainian boy and his family leave cellar after 87 days for safety abroad

'Devil's advocate'? / Russian soldier's Ukrainian lawyer defends role on eve of verdict

Headlines

Australian e… / Labor incre… likely to form majority government Liberals desc… into turmoil

Anthony Albanese a… team will be sworn i… Monday as PM-elect… wants to 'change the…

Sky News In shock a… Liberal defeat, comm… party to shift right

Monkeypox / UK to announce more cases as efforts ramp up to contain outbreak

US Biden says 'everybody' should be concerned about spread of monkeypox

Arkansas / Republican admits abortion trigger law would cause 'heartbreak' if Roe is reversed

Privacy settings

Please manage your cookie choices by switching the consent toggles on or off under the Purposes listed below. These cookies will be stored based on your consent choice, but may also use the personal data they collect when we or our third party partner has a legitimate interest.

You can see details of these legitimate interests, including links to the relevant privacy policies, and have the right to object to the use of your data in the "Legitimate Interest" section below. You can also choose to click:

Reject all   Accept all

Purposes | Features | Site Vendors

User Consent | Legitimate Interest

Purposes

Select 'On' if you are happy for us to use your data for the following Purposes. You can also make individual Vendor choices under each Purpose.

Custom Purpose (C) = Custom Purpose

⌄ Store and/or access information on a device   Off On

⌄ Personalised ads and content, ad and content measurement, audience insights and product development

Status: Rejected All   Off On

Special Purposes

We use your data for these purposes so we can deliver our services to you

⌄ Ensure security, prevent fraud, and debug

⌄ Technically deliver ads or content

⌄ Guardian Essential Cookies
Custom Purpose (C)

⌄ Other Essential Cookies
Custom Purpose (C)

You can change the above settings for this browser at any time by clicking the privacy settings link in the footer of the page.

Save and close   Cancel

Remember cookies?

Your browser is a “smart hub” running 3rd party code (html + JS + Wasm)

Web services request access to your data

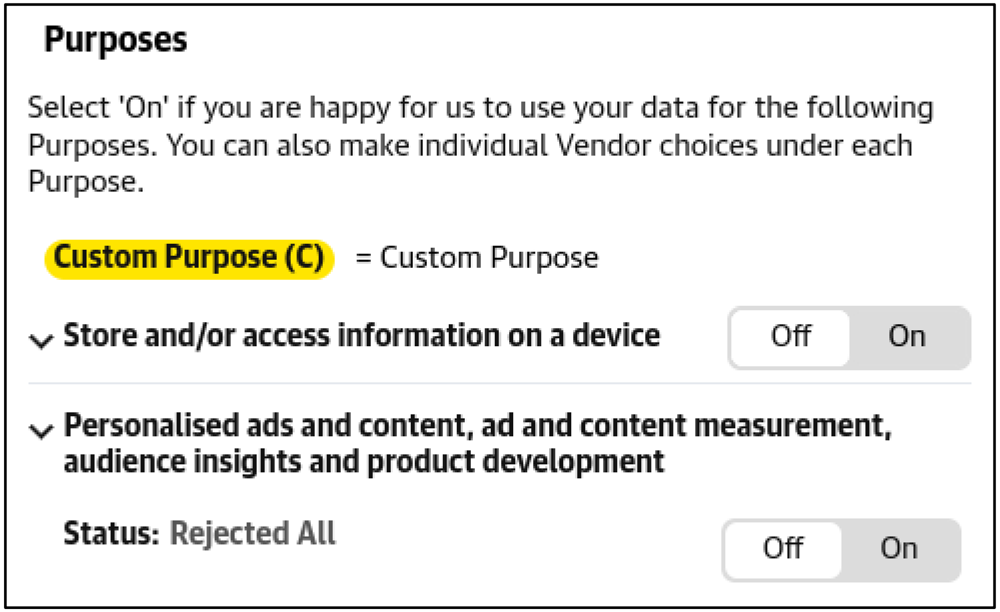
Services provide purpose description

You can allow/reject based on your own privacy-vs-utility assessment

Your choices are registered and enforced*

You start using the desired service

Some of your data is processed right in a browser, other is sent to the server.



Purposes

Select 'On' if you are happy for us to use your data for the following Purposes. You can also make individual Vendor choices under each Purpose.

Custom Purpose (C) = Custom Purpose

Store and/or access information on a device — Off / On

Personalised ads and content, ad and content measurement, audience insights and product development

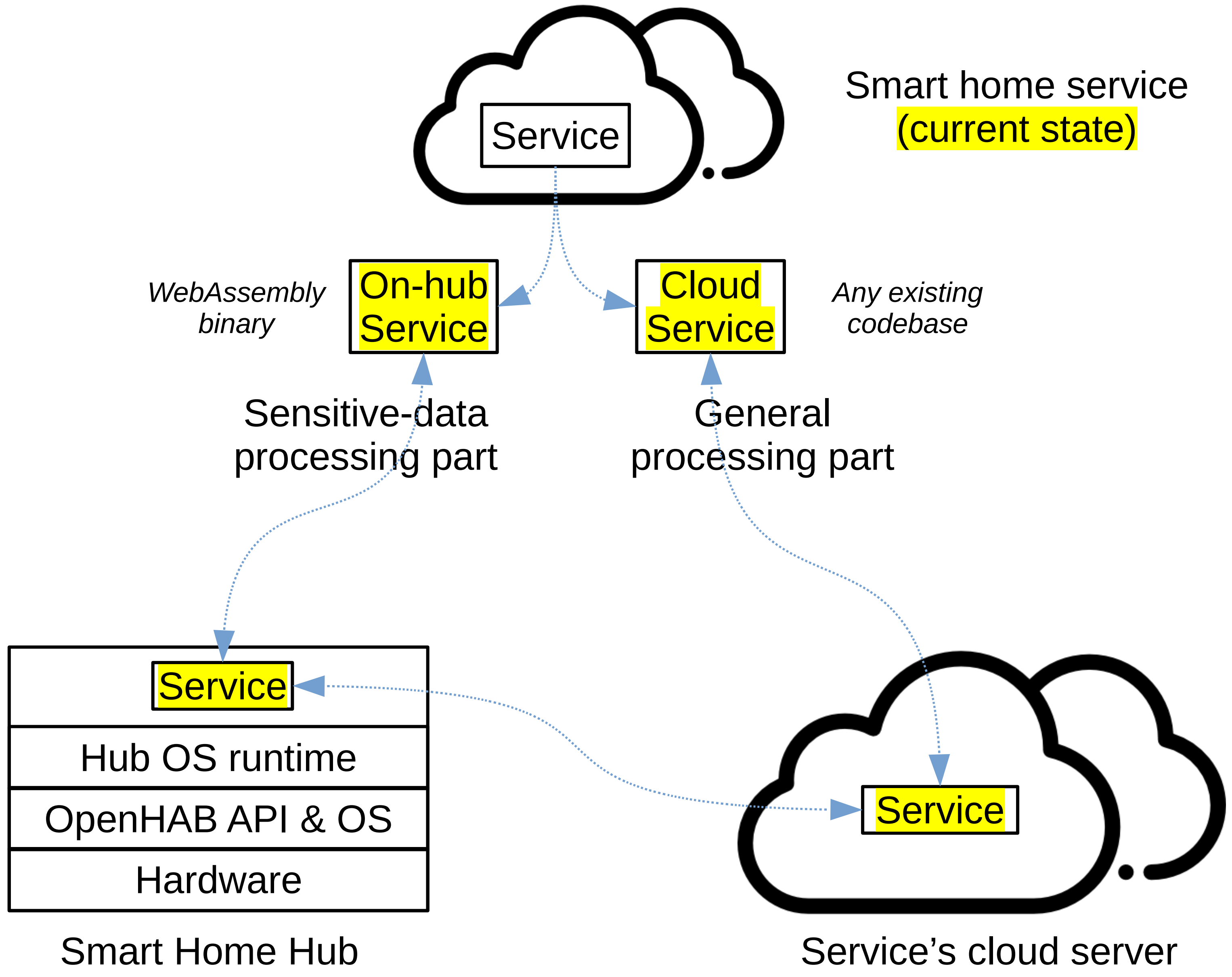
Status: Rejected All — Off / On

efficiency of this enforcement is a topic for another seminar

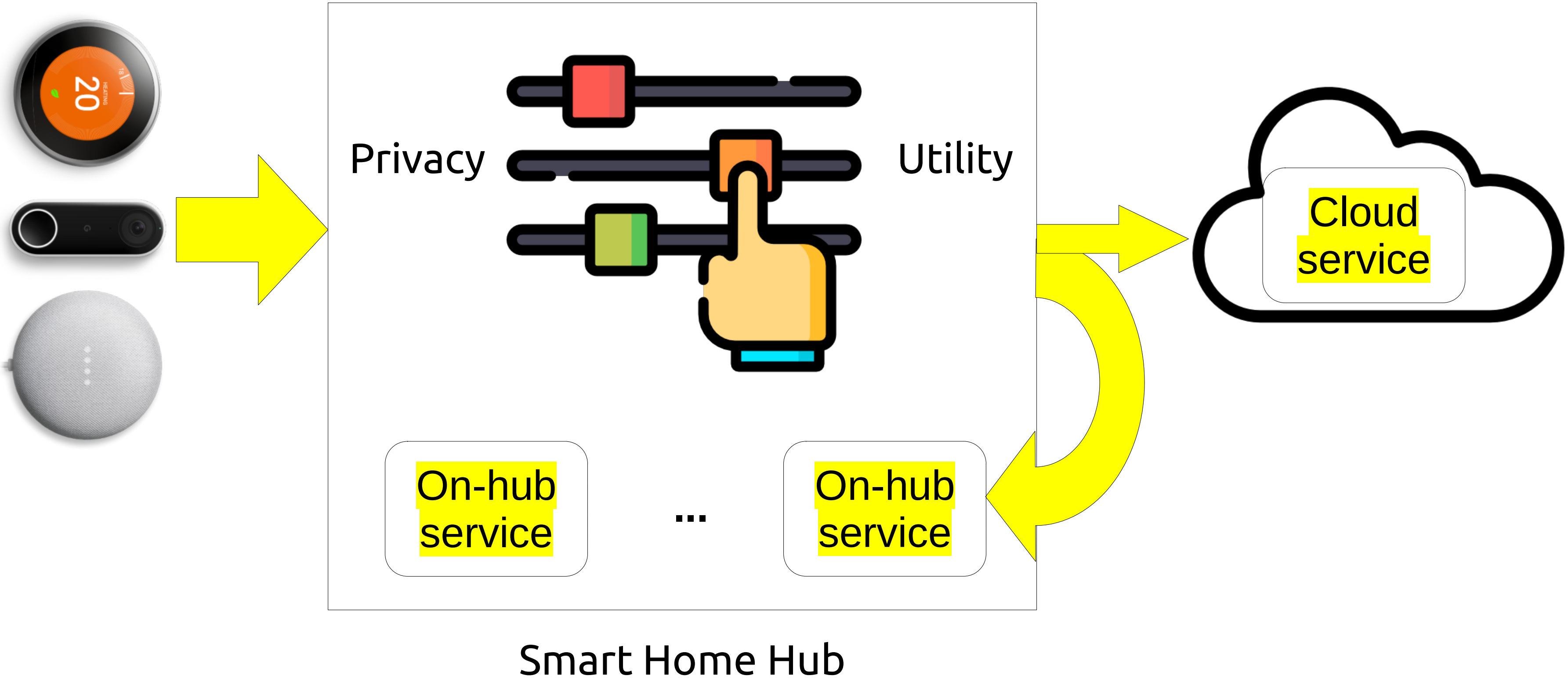
HubOS

- Privacy-oriented OS for smart hubs
- Allows smart home services to access sensor data for a given purpose (see cookies request)
- Users define how and where their sensor data is processed (at the hub, cloud, or both)
- HubOS provides runtime for on-hub processing: access control, installation, execution, sandbox, network, fs, …
- WASM format for on-hub code

HubOS deployment



HubOS big picture



References

HomePad

Zavalyshyn, Igor, Nuno O. Duarte, and Nuno Santos. "HomePad: A privacy-aware smart hub for home environments." 2018 IEEE/ACM Symposium on Edge Computing (SEC). IEEE, 2018.

PatrIoT

Zavalyshyn, Igor, et al. "My House, My Rules: A Private-by-Design Smart Home Platform." MobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. 2020.

SoK: Privacy-enhancing Smart Home Hubs

Igor Zavalyshyn, Axel Legay, Annanda Rath, and Etienne Riviere, “SoK: Privacy-enhancing Smart Home Hubs”, The 22nd Privacy Enhancing Technologies Symposium (PETS), July 11–15, 2022, Sydney, Australia