Privacy by Design beyond the screen
Some notes from a recent workshop

Tjerk Timan, TILT, UvT, t.timan@uvt.nl

before I start...

this happened…

Trump to deliver verdict on Paris climate deal as world fears US pullout

The president has reportedly made his decision on the landmark climate deal, as exasperated world leaders get ready to move on with or without the US

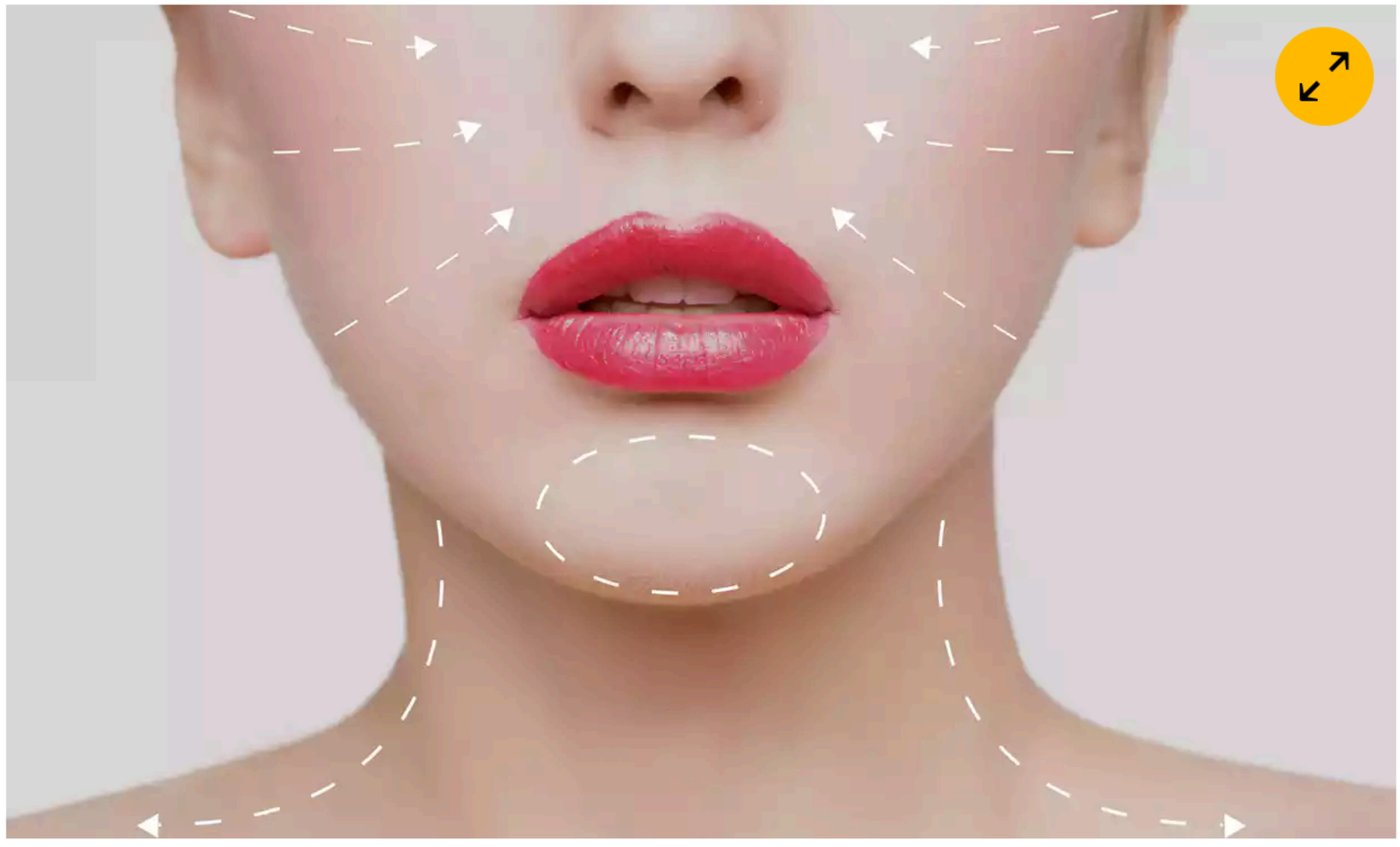
Donald Trump with Angela Merkel and Tunisian president Beji Caid Essebsi at the G7 summit. Merkel said: 'The whole discussion about climate has been difficult, or rather very unsatisfactory.' Photograph: Flavio Lo Scalzo/AP

so, let's skip the '*data is the new oil*' metaphor, shall we?

this ALSO happened…

Hackers publish private photos from cosmetic surgery clinic

Criminal group that broke into servers of Lithuanian clinic demands bitcoin ransom payments from clients after releasing 25,000 pictures



More than 1,500 British patients are listed in the database. Photograph: kopitinphoto/Getty Images/iStockphoto

So.. data does leak and gets stolen etc…
But is that REALLY about privacy?
> Main question (what is) privacy **beyond** data protection?
> Or does data protection go **beyond** **classical** privacy protection?
> privacy as a **right** and as a **value**
> **data ‘control’** as a right and **as a value**?
> isn’t it just about **‘data ethics’**
> but then, how can we implement **THAT**?

privacyspaces

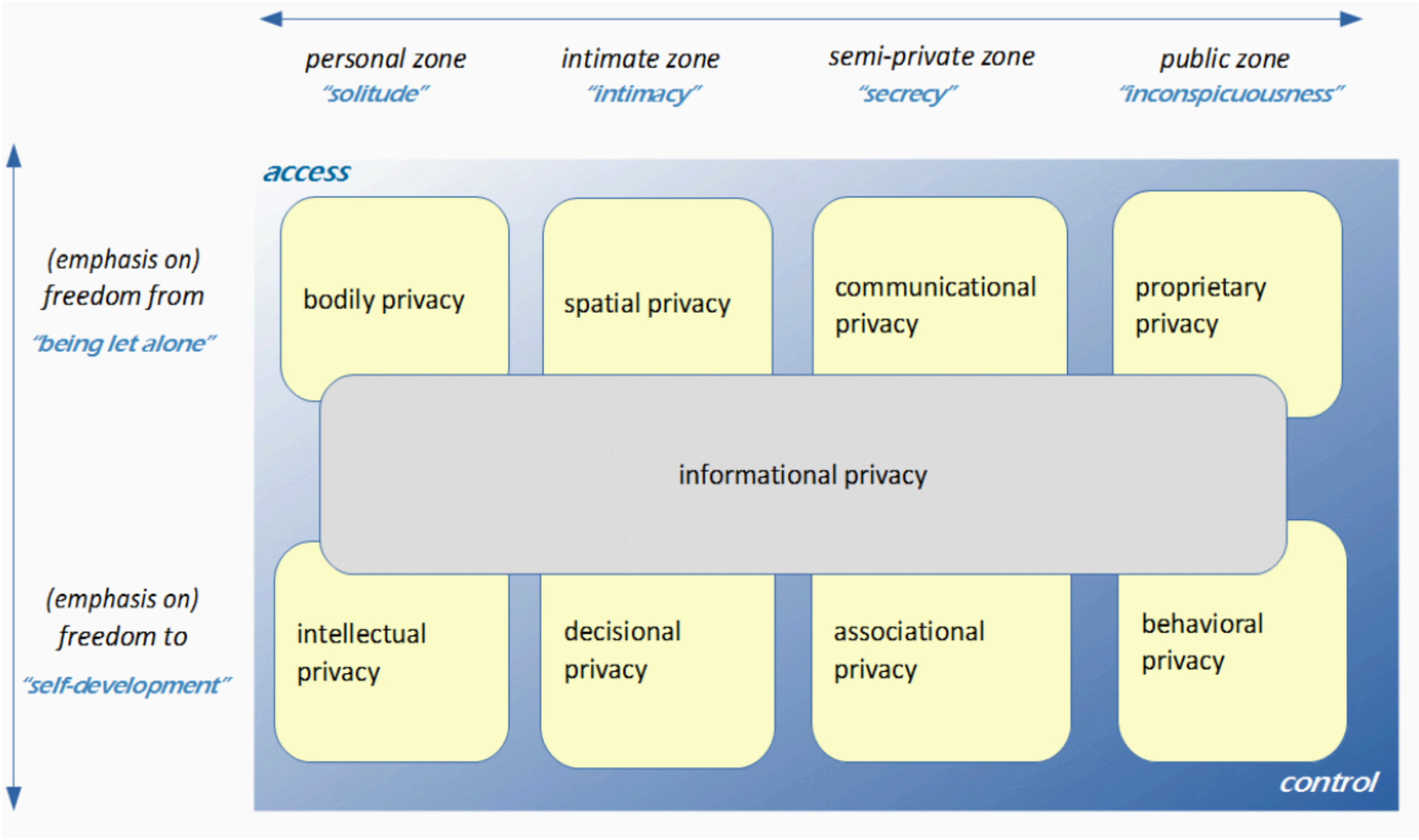
CPDP 2017 session on a typology of privacy

admin

We had a great session and some heated debates on privacy typologies at the CPDP 2017 conference in Brussels! Watch the video below. Thanks again [...]

READ MORE

A Typology of Privacy



Privacy by Design beyond the screen
Some notes from a recent workshop

Tjerk Timan, TILT, UvT, t.timan@uvt.nl

> PbDBtS
> main challenges
> what did we do?
> some outcomes and directions

Privacy By Design

> from set of **principles** to concrete **tools**
> **building** privacy **into** the technology
> as a **product** or a **process**
> also, it will be a **legal** requirement / instrument

> what does PbD mean?
  > **depends** on who you ask….
  > we have to look for ‘best’ practices:


zlglass.en.afibaba.com
on

Portland

Public

Post

Privacy Checkup

Skip

Hi Sam — Sorry to interrupt. You haven't changed who can see your posts lately, so we just wanted to make sure you're sharing this post with the right audience. (Your current setting is Public, though you can change this whenever you post.) Learn more.

Who do you want to share this post with?

Friends	Public	More Options

"DNS,10.0.1.101,2219,1489170337,dowse.it,.

3/10/2017, 7:25:37 PM node: deb

dns-query-channel : msg.payload : string[43]

"DNS,10.0.1.101,2220,1489170337,dowse.it,.

3/10/2017, 7:25:49 PM node: deb

dns-query-channel : msg.payload : string[43]

"DNS,10.0.1.101,2221,1489170349,dowse.it,.

3/10/2017, 7:25:49 PM node: deb

dns-query-channel : msg.payload : string[52]

"DNS,10.0.1.101,402,1489170349,google.com,

3/10/2017, 7:25:51 PM node: deb

dns-query-channel : msg.payload : string[55]

"DNS,10.0.1.102,85,1489170351,facebook.com

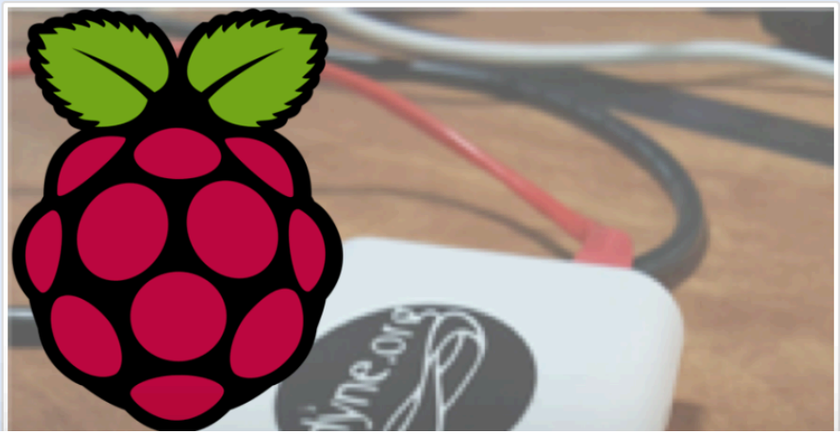
3/10/2017, 7:25:52 PM node: deb

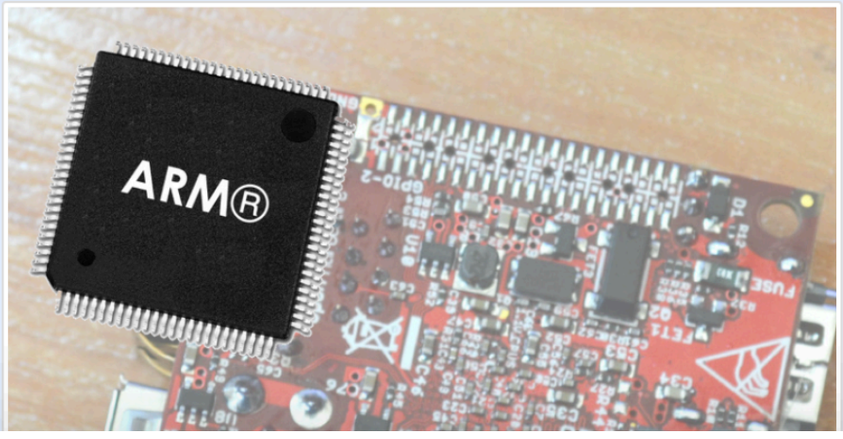
COMMUNITY OWNED NETWORKS

WERE YOU CAN SEE WHAT IS GOING ON

NEGOTIATE ACCESS AND REACT

Dowse 1.0 beta is out!





physical privacy ——— hybrid privacy ——— data protection

‘doing’ something ——— capturing ‘doing’ ——— manipulation of records

influence on real world ← sensor/ actuator ← feedback to context

.. we need more best-practices…

Reminder: principles as put by Cavoukian

1. Proactive not reactive; Preventative not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality – positive-sum, not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric

What and where can PbD be?

> privacy within the **design process**
> PbD as a **legal** requirement
> as **organisational** ‘awareness’
> as **policy** statement
> as a part of user/ **market research**
> as competitive **advantage**
> as a **transparency** document/ activity
> etc…

Some concerns of PbD in practice

> **I - methodology** (or, blame the designers (again))
> Lack of possibilities to **protest** in the Digital (Galloway's protocol-argument)
> **Too-big-to-fail** intermediaries (powerlessness argument)
> Values and **relativism** (privacy is flexible)
> re/de-identification (data protection techniques) **not sufficient**
> design- and **coding practices** are not so easily adaptable and/or controllable (applicability and enforcement argument)

Status Photo Place Life Event

What's on your mind?

feeling How are you feeling?


happy


sad


tired


great


wonderful

Some more concerns

> privacy by design:
> already **difficult**
> moving from **front-end** and user control to **back-end** and information architecture
> privacy-by-default

> models of consent and settings: **rational ‘tweaking’ of variables** irt privacy (mainly data sharing and data protection)

> completely **useless** in phenomena such as smart CCTV **reading your face** from a distance or when a smart toy is **influencing the behavior** of a child


touchless

PbDBtS

> privacy by design **beyond the screen**
> what happens when interaction with ICTs moves beyond **text** and **screen-based** interfaces
> sensing and actuating system without user input
> human as a **data generator** by default
> smart environment with increasing NUS
> user friendly and smooth, but at the loss of understanding or **grasping why**

Interaction with ICTs

> start: code- and **rule- based**
> Graphical User Interface **(GUI)**
> Tangible User Interface **(TUI)**
> **Natural** User Interface (horrible term!)
> to move **away from the computer** and into more ‘easy’ flows between input, processing and output
> interaction **!= always** information or data, or is at least more subtle that discrete in- and output

from code and text:

```
A:dir
COMMAND  COM     4896   8-23-83   1:15a
FORMAT   COM     2688   1-01-80   1:01a
RECV     EXE     1024   8-23-83   1:02a
DEBUG    COM     6016   8-22-83   3:05p
CHKDSK   COM     1728   8-22-83   3:00p
FILCOM   COM     8320   8-22-83   3:03p
EDLIN    COM     2432   8-22-83   3:06p
LINK     EXE    41856   8-22-83   3:13p
EXE2BIN  EXE     1280   8-22-83   3:07p
MASM     EXE    70784   8-22-83   3:21p
SYS      COM      608   8-22-83   3:23p
FORMAT   OBJ     4224   8-22-83   3:25p
CREF     EXE    13824   8-22-83   3:02p
LIB      EXE    32128   9-20-83   2:18p
RDCPM    BAK     1920   9-20-83   2:19p
RDCPM    COM     9600   9-20-83   2:20p
RDCPM    OBJ      132   1-01-80   1:04a
      17 File(s)
A:
```

to visual manipulation and cartesian space:

to the first GUI
(graphical user interface):

Desk File/Print Edit Type Style Page Layout Arrangement Fill Lines Pen

Undo Last Change

Cut ⌘X
Copy ⌘C
Paste ⌘V

Clear
Duplicate ⌘D
Select All ⌘A

Make Lowercase
Make Uppercase
Make Title

Reshape
Smooth
Unsmooth

Round Corners...

LisaWrite Paper
LisaTerminal Paper
Clock
Template
Face
LisaGraph Paper
Peggie's Rose
Text
Calculator
0
285714286
M− M+ Mx
M÷
√x
MR
Clock
Preferences
WasteBasket
ClipBoard
DTC Paper
Calculator
-ProFile
-Widget

to the notion of the TUI
(tangible user interface):

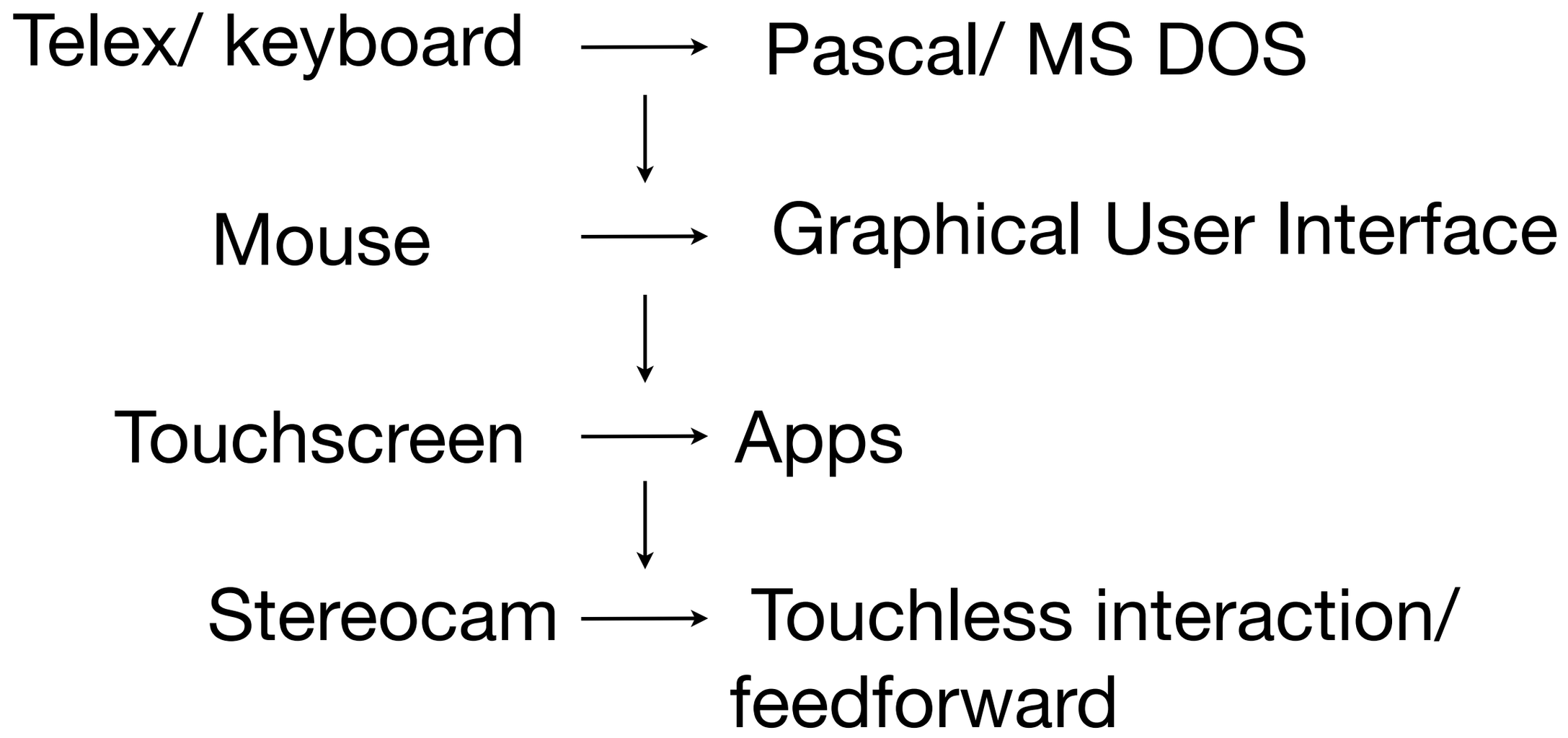
(naive) design thinking

>**user-centerer** design
>first ideas of **co-design** and including stakeholders
>thinking **beyond the limits** of the GUI and the screen

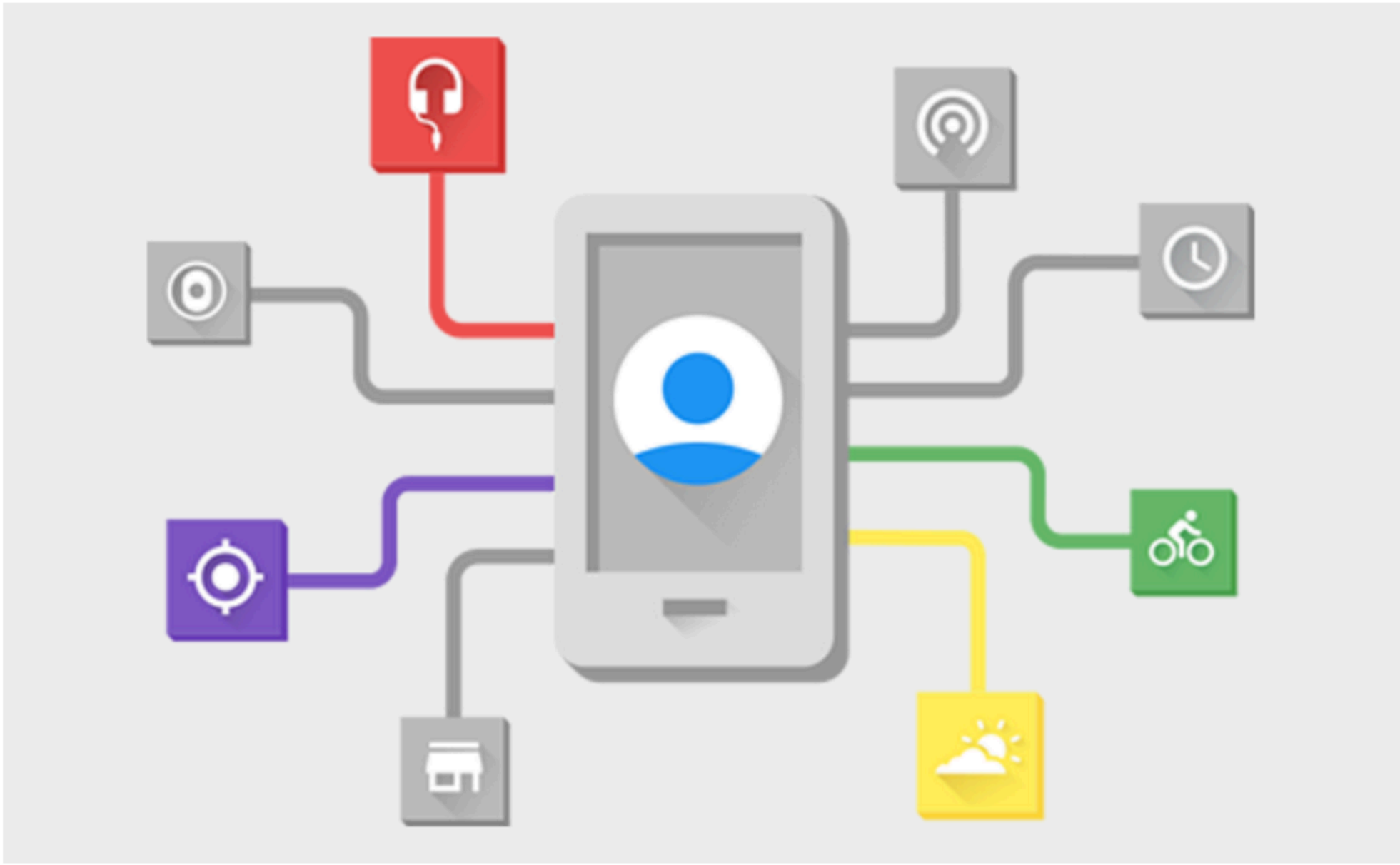
(naive) design thinking

> aimed at **changing** social systems
> technological solutions for **social problems** (very idealistic)
> high belief in technology **progressing**
> **playing** between the digital and the physical
> search/ quest for **platforms for “IoRT”**

an overview


Telex/ keyboard
Pascal/ MS DOS
Mouse
Graphical User Interface
Touchscreen
Apps
Stereocam
Touchless interaction/
feedforward

Combine signals with the Awareness API



The Awar
started w
Access 7
that is sin
Combine
experienc
their curre
their cont

GET START

networks of things?

internet between **PC's** (darpanet)

↓

internet of **devices** (mobile & comp)

↓

internet of **things** (cognisphere, networked objects)

↓

internet of **bio** ... things?

current design rationale:

> persuasive - **nudging** - default settings

> renewed focus on smart objects as **external sensors** for smarthones

> because **unknown category,** the design is blobby, shapeless, undefined


PHILIPS
11 9354 2009
LIGAR

Main challenges workshop

> to discuss **if and how PbD is possible** in smart-connected environments, in which we interact with system in beyond a textual and visual way

> to explore PbD in a **near-future** using 2 scenarios

> **smart toys** in the home
> **augmented reality** glasses in public space

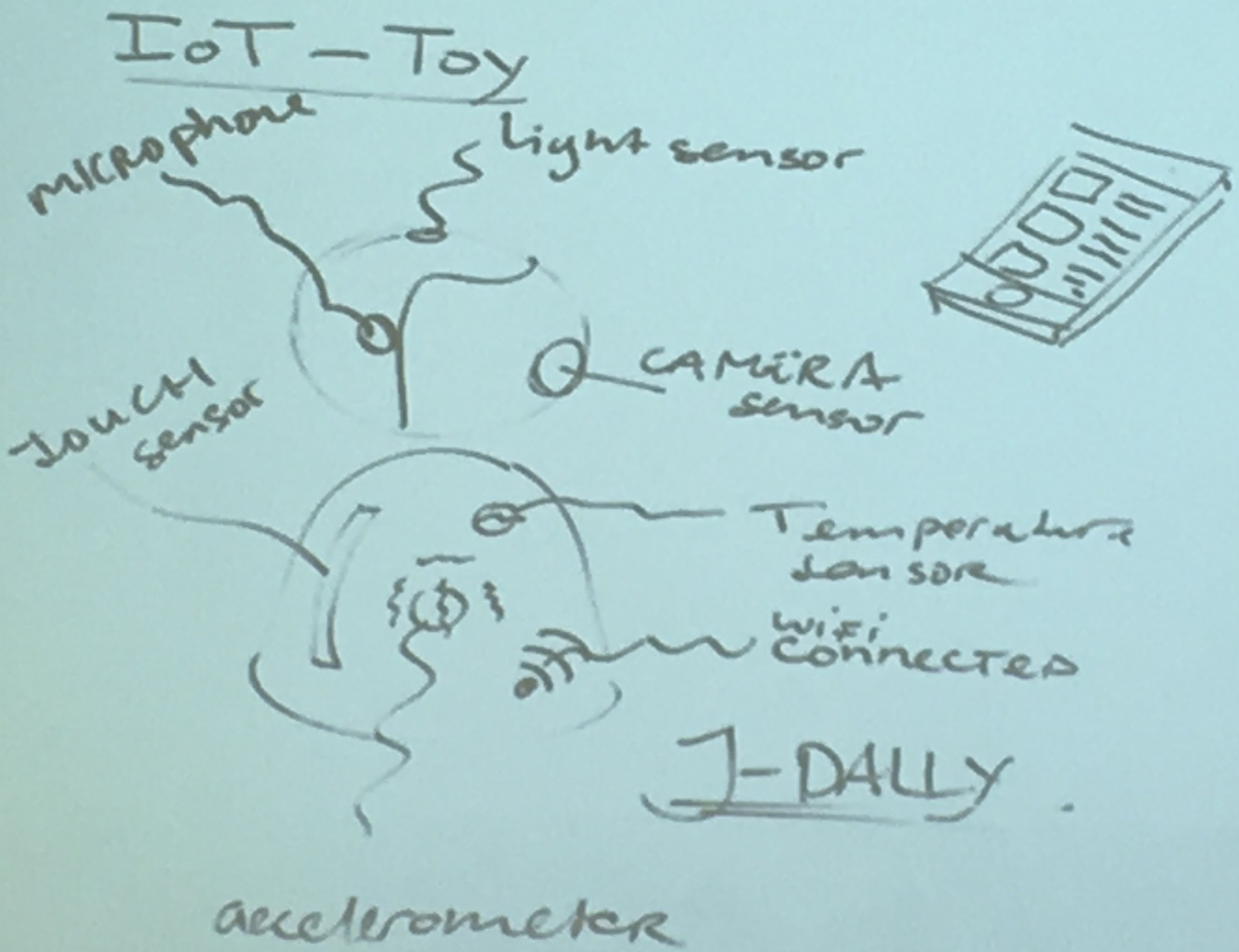
What did we do?

> Inform each other on PbD from **different disciplines** (computer science, design, law, ethics)
> Develop ideas **through scenarios** via multidisciplinary teams in ‘break out sessions’
> Write and draw **on the walls**!
(because the Lorentz-centre affords it!)

Scenario 1: Smart Toys

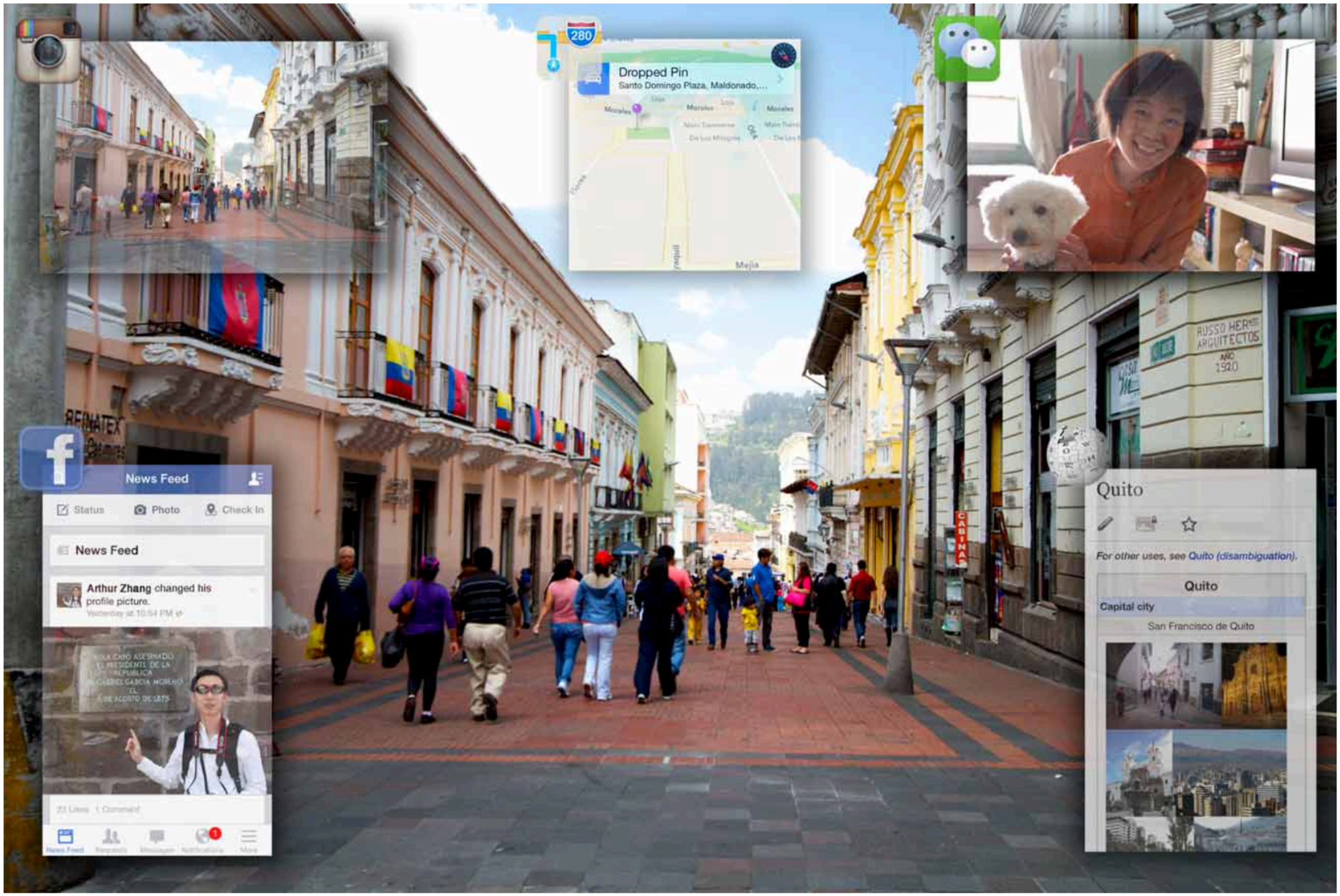
(the VaiKai connected doll, see https://vaikai.com/)

J-DALLY



Patterns of Life

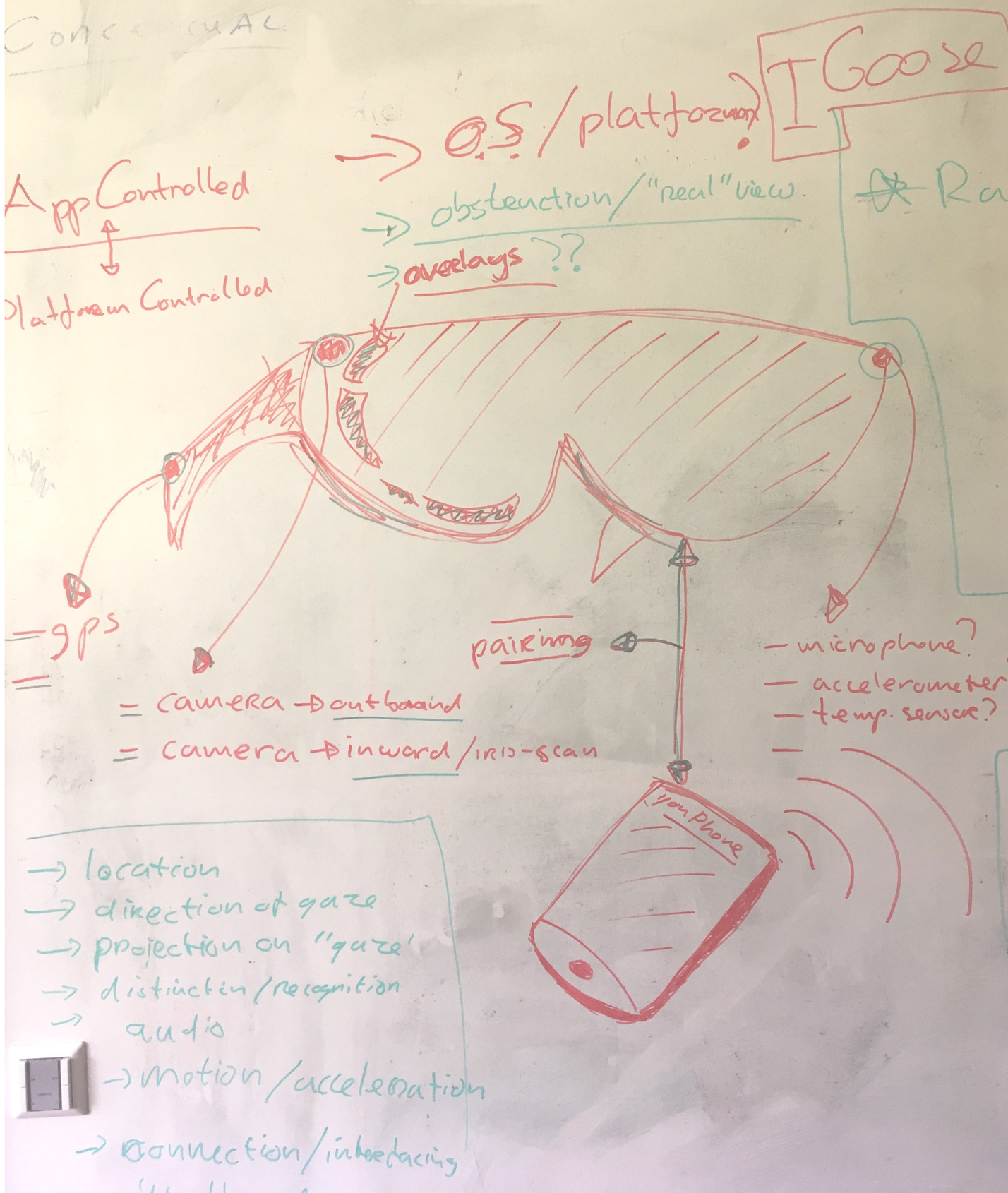
Scenario 2: Augmented Reality



(concept picture for an augmented reality lens, see https://www.sammobile.com/2016/04/05/samsung-is-working-on-smart-contact-lenses-patent-filing-reveals/)

iGo

Liberating your view on reality



main take-aways

PhD as a process

PhD as a product

Random remarks:

research Q's

Policy recommendations


PANORAMA
App Controlled
O.S/platform
IGoose
Platform Controlled
overlays
gps
= camera-outboard
= camera-inward/iris-scan
pairing
microphone?
accelerometer?
temp sensor?
location
direction of gaze
audio
motion/acceleration
cloud-based
Bio Sensors
Body Area Network
Rainbow Glasses
IGo
weNo
dayNo
To Do
OBJECTIVES
ACTIVITIES
OUTPUT
real-time warrant
screaming
Privacy
all this data is recorded...
will it be deleted? yes
store
delete/purge
hotlist
NETWORK ANALYSIS
Third Party Doctrine

Definition	Design Solution
The right to be let alone because: the first definition ever read, seems accurate in many respects.	Don't get on the interwebs
Privacy is the right to be treated fairly. "Doe effe normaal" - shortest possible rule for privacy a certain lawyer could come up with. The actual threat comes from unintended use of the data.	A system should behave the way you expect that.
A space time coordinate where I can be myself.	Control on flow of people and information through (locked) doors and 'holes' in the house.
Freedom from judgement of others.	The design of the information system should allow for understanding, explaining, correcting or bypassing desicions (... etc.) of the system.
Intimacy (Still a problem, a lot of pressure to break through these boundaries. And this has not been adressed yet by technology.)	Individual control
Privacy shields individuals from unwanted exposure in order to restrict the domination of one agent over another and(..check with B to complete this note or see a picture)	The right to be left alone. + expression
Don't get near to any connected device? Any technology hides consequences that you cannot see.	Having room to be yourself. - inspired by: The freedom from unreasonable constraints on the construction of your identity (Phil Agre). The room/house/space is still around you. Bubbles;

	extended self.
The freedom from unreasonable constraints on the construction of your identity. (Links privacy with identity; identity as selfhood. About the process of construction. ps. You cannot have any freedom without constraints.)	Have designers of information systems be aware of privacy.
Contextual integrity. Nissenbaum; the context of the end-user is important to take into account.	Transaction without documentation.
(Contextual integrity)^2 because its both abstract and observational.	Understand risks and put in place appropriate safeguards.
Following personal information whenever (?in motion?)	User friendly design, boundaries.
Control of ones personal sphere - because it was sufficiently vague.	Define personal sphere; full configuration of personal sphere....
The freedom from unreasonable constraints on the construction of your identity (Phil Agre) - Chilling effect; being put into bubbles, concerns are profiling tracking.	Stop tracking. Control over datasets that have normalizing chilling effects.
Right and freedom to be let alone (Protect this despite context.) Design Solution: To be able to shut 'it' down. Adapt the (settings of the) system at all times.	
Contextual Integrity. Because upperclass english gentleman say: don't read eachothers e-mail.	Find back some civility. The patterns of my life need to be stored locally on me, only need to be available on a "need to have" basis.
Control on the context flow of personal information. (Inspired by Nissenbaum/ Nissenbaum helps people to understand why infringements on privacy 'feel bad'.)	ZK proofs on every interaction +/ Secret only at the user. - Won't work was just first guess.

What PbD should NOT be/do

> Focus on data minimization (distracts from the real problems) ****

> Privacy is not sufficient, this is about power/ politics/institutions/societal principles *****

> Don’t ignore infrastructure and political economy ****

What PbD SHOULD be/do

> Integration into hardware dev. process? *******

> We need concrete/practical examples of PbD implementation (to function as guidance)****

> PbD evaluation techniques (level of protection + security + user cognition + …) ***

> Making privacy visual / tangible – you see/feel your personal data flowing out of your phone & returning in the form of ads etc.***

Some outcomes and directions

> PbD seems **impossible** in the context of smart environments (due to uncontrollability of interactions and data flows between humans and machines)

> **by-stander** privacy hard to protect

> **too many values** come into play when talking PbD - maybe we have to go back to **PET's**?

> PbD as a product **no**, as a process **maybe**

Solutions from a life cycle perspective

- Making use of the smartness of the toy
  - dynamic consent
  - the doll explaining the privacy policy
  - three monkeys (don't speak, don't listen, don't see)
- blurring of bystanders
- blurring of private parts

Some outcomes and directions

Some open questions of IoT and smart environments irt PbD:

> **life cycle** of data and product (smart doll)
> **new** mediated **interactions** - not sure yet how it will be accepted (glasses)
> **AI** can help control and manage, or block but is seems **after-the-fact**
> via **fines** and **enforcement** (seems most promising, yet not very imaginative)
> PbD - necessary to define its limits (**what it is not**)
> it is not about big data, it is about '**situational awareness**' in an actual space of such devices

> Should PbD be a **set of methods**, techniques, principles, protocols, or a general ‘stance’?
> Should we **still talk about** Privacy By Design?
> How much is **‘by design’** an obfuscation?
> Where can we **draw boundaries** of PbD
> How to assess its ’success’ and who should do this?
> Is **education** and awareness **enough**?
> Shouldn’t we **let go of PbD** and rather talk of **Responsible Innovation** (allowing for a broader set of values)
> shouldn’t we just speak of **data ethics**?