Cookie in the Fridge

privacy problems with the Internet of Things and some ideas how to fix them

Greg Alpar

gaa@ou.nl   www.open.ou.nl/gaa

Open University, Radboud University

19 November, 2016   TouW Symposium

Who are these companies?

Agenda

- **IoT and people**

- Central and linkable data processing

- Attributes in IoT

- Conclusion

Internet of Things

IoT is "the interconnectivity of our digital devices that provides endless opportunities for brands to listen and respond to the needs of their customers – with the right message, at the right time, on the right device".
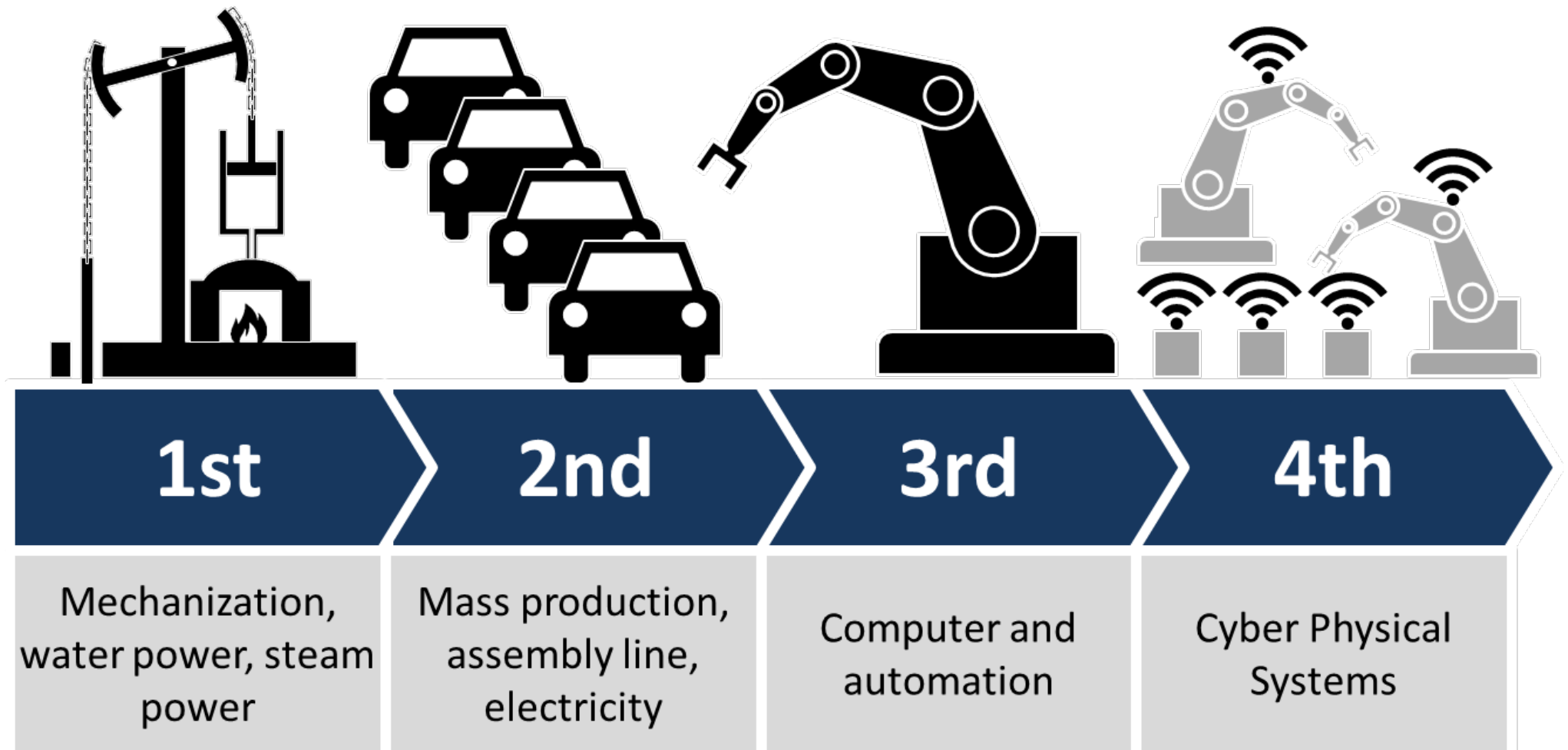
(Marketo, 2016)

Internet of Things

IoT is "the interconnectivity of our digital devices that provides endless opportunities for brands to **listen** and **respond** to the needs of their customers – with the right message, at the right time, on the right device".

(Marketo, 2016)

1st	2nd	3rd	4th
Mechanization, water power, steam power	Mass production, assembly line, electricity	Computer and automation	Cyber Physical Systems

G. Alpar (OU), TouW Symposium, 19-11-2016
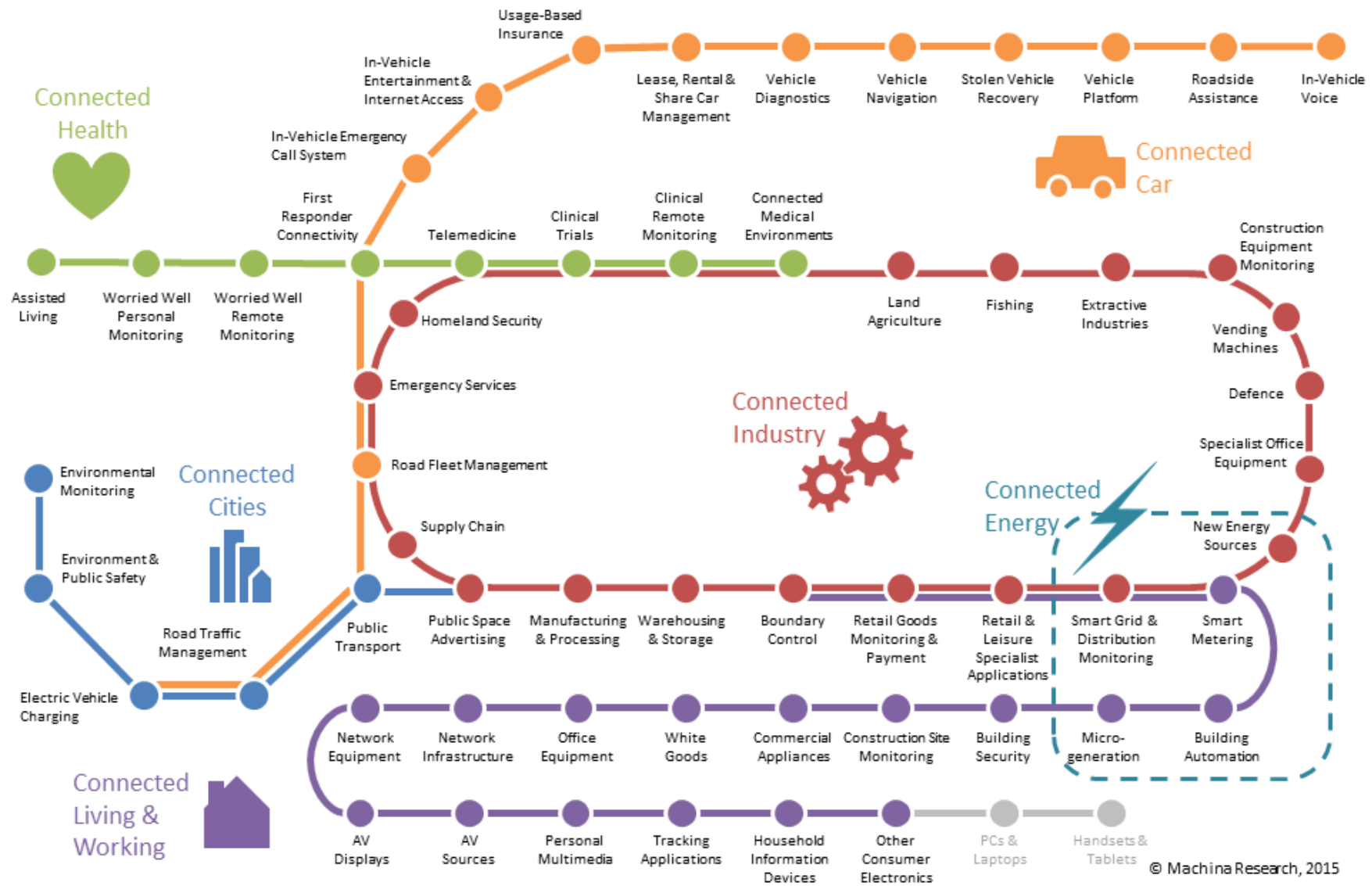
Standardisation efforts

- IPv6

- Reference architectures
  - IoT-A
  - IIRA
  - RAMI 4.0

- Standards:
  - NIST SP 800-183 *Networks of 'Things'*, July 2016
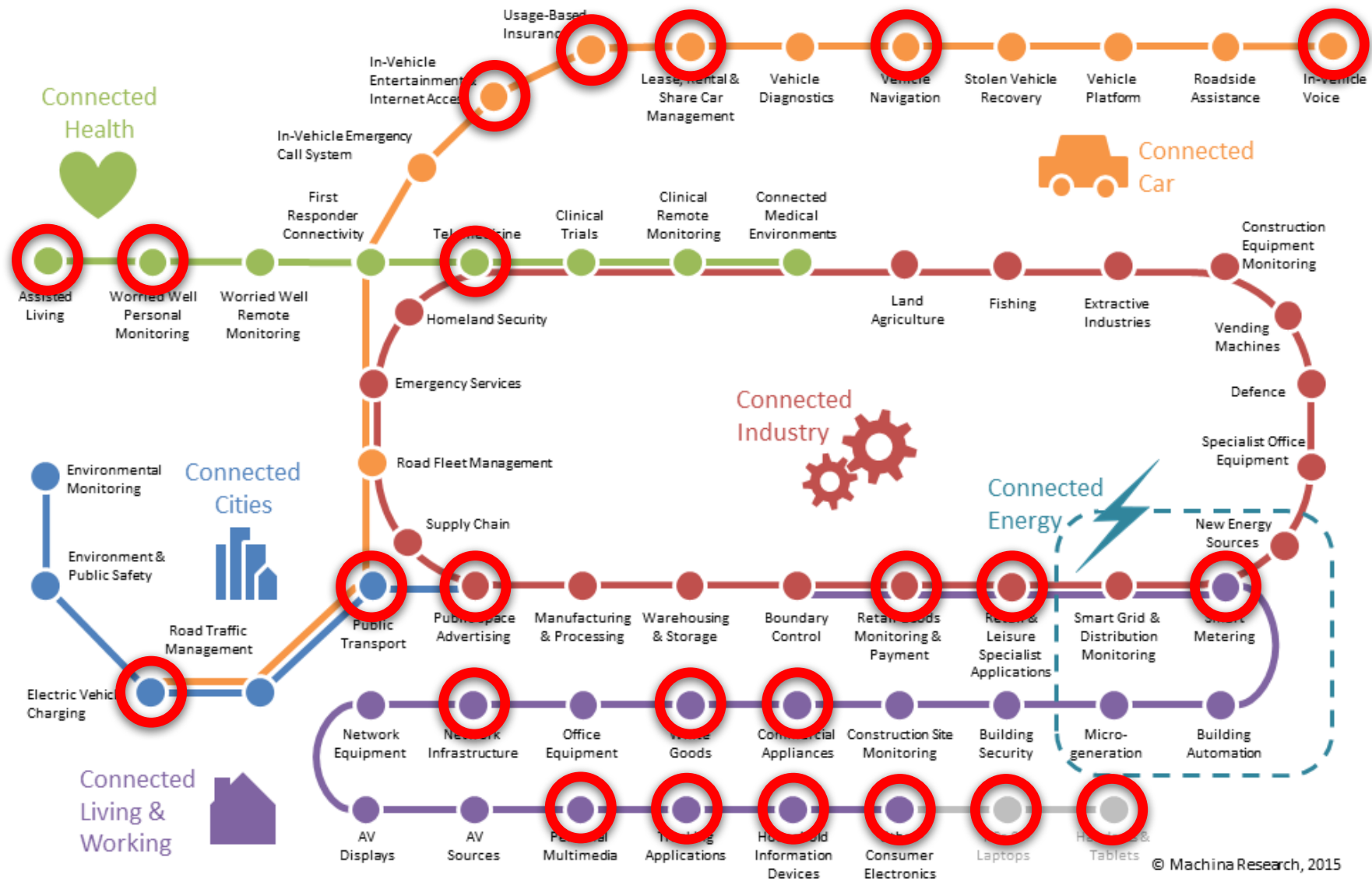 - IEEE P2413 *Architectural Framework for the IoT* (ongoing project)

Recent industrial boost

- Google: Brillo OS and Weave communication

- Microsoft: Windows 10 supports IoT

- Samsung: design of new IoT chips

Connected Health

Connected Car

Connected Industry

Connected Energy

Connected Cities

Connected Living & Working

Assisted Living — Worried Well Personal Monitoring — Worried Well Remote Monitoring — First Responder Connectivity — Telemedicine — Clinical Trials — Clinical Remote Monitoring — Connected Medical Environments

In-Vehicle Emergency Call System — In-Vehicle Entertainment & Internet Access — Usage-Based Insurance — Lease, Rental & Share Car Management — Vehicle Diagnostics — Vehicle Navigation — Stolen Vehicle Recovery — Vehicle Platform — Roadside Assistance — In-Vehicle Voice

Homeland Security — Emergency Services — Road Fleet Management — Supply Chain

Land Agriculture — Fishing — Extractive Industries — Construction Equipment Monitoring — Vending Machines — Defence — Specialist Office Equipment — New Energy Sources

Environmental Monitoring — Environment & Public Safety — Road Traffic Management — Electric Vehicle Charging — Public Transport

Public Space Advertising — Manufacturing & Processing — Warehousing & Storage — Boundary Control — Retail Goods Monitoring & Payment — Retail & Leisure Specialist Applications — Smart Grid & Distribution Monitoring — Smart Metering

Network Equipment — Network Infrastructure — Office Equipment — White Goods — Commercial Appliances — Construction Site Monitoring — Building Security — Micro-generation — Building Automation

AV Displays — AV Sources — Personal Multimedia — Tracking Applications — Household Information Devices — Other Consumer Electronics — PCs & Laptops — Handsets & Tablets

© Machina Research, 2015

G. Alpar (OU), TouW Symposium, 19-11-2016

Connected Health

Connected Car

Connected Industry

Connected Energy

Connected Cities

Connected Living & Working

Assisted Living
Worried Well Personal Monitoring
Worried Well Remote Monitoring
First Responder Connectivity
In-Vehicle Emergency Call System
In-Vehicle Entertainment & Internet Access
Usage-Based Insurance
Lease, Rental & Share Car Management
Vehicle Diagnostics
Vehicle Navigation
Stolen Vehicle Recovery
Vehicle Platform
Roadside Assistance
In-Vehicle Voice

Telemedicine
Clinical Trials
Clinical Remote Monitoring
Connected Medical Environments
Land Agriculture
Fishing
Extractive Industries
Construction Equipment Monitoring
Vending Machines
Defence
Specialist Office Equipment

Homeland Security
Emergency Services
Road Fleet Management
Supply Chain
Manufacturing & Processing
Warehousing & Storage
Boundary Control
Retail Goods Monitoring & Payment
Retail & Leisure Specialist Applications
Smart Grid & Distribution Monitoring
New Energy Sources
Smart Metering

Environmental Monitoring
Environment & Public Safety
Road Traffic Management
Electric Vehicle Charging
Public Transport
Public Space Advertising

Network Equipment
Network Infrastructure
Office Equipment
White Goods
Connected Appliances
Construction Site Monitoring
Building Security
Micro-generation
Building Automation

AV Displays
AV Sources
Personal Multimedia
Tracking Applications
Household Information Devices
Consumer Electronics
Laptops
Handsets & Tablets

© Machina Research, 2015

G. Alpar (OU), TouW Symposium, 19-11-2016

Agenda

- IoT and people

- **Central and linkable data processing**

- Attributes in IoT

- Conclusion

Target story

- Assignment: find pregnant women in their 20th week
  - Typical products: unscented lotion, Mg, Ca, Zn
- Target sends coupons
- Father upset: "My daughter got this in the mail! She's still in high school, and you're sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?"
  - Later the father: "I had a talk with my daughter, it turns out there's been some activities in my house I haven't been completely aware of. She's due in August. I owe you an apology."
- Target's conclusion: personalised ads are a mix of products for pregnant women and unrelated items
  - "an ad for a lawn mower next to diapers", "a coupon for wineglasses next to infant clothes"
  - "That way, it looked like all the products were chosen by chance."

http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Lessons learnt

- Better targeting people helps sell more
  - That is, raise the profit

- Companies have to be smart not to upset people
  - More surreptitious practices?

- It feels arguably odd that our **behavioural information** gives away so much about our private matters

AOL fiasco in 2006 – demo

http://www.not-secret.com
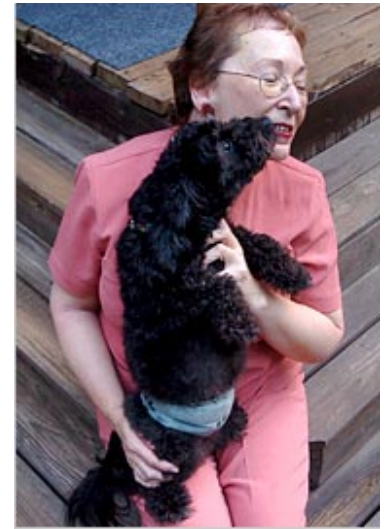
Lessons learnt

- What we search can reveal a lot about us
  - Often it can be embarrassing

- Even a huge company can make stupid things
  - Often huge companies store our personal data

- Anonymity ≠ privacy
  - See also Netflix (2008)
  - Our activities can still be *linkable*

Cookies – a bit of history

- HTTP: no memory (1991)

- Memory mechanism is needed (Lou Montulli, 1994)
  - Without traceability

- *Cookie*: a small file only accessible by the web server that created it in a browser (Netscape)

- HTML page can contain components from various web servers

- *By a **third-party cookie**, a web server can link various web-site visits of a user*

http://www.montulli-blog.com/2013/05/the-reasoning-behind-web-cookies.html

Cookies – uncomfortable decision

- Lou's "uncomfortable decision": keep third-party cookies
    1. Publicly visible companies
    2. If 3rd party cookies were disabled, businesses would find other, more surreptitious, mechanisms

- Result: cookies exist but with more transparency (visibility, control)

- But now: we don't really know most tracking and advertising companies and there do exist more surreptitious mechanisms

Cookies – demo

WHAT'S NEW

The new … app is here—and it's all about making your … experience faster, smarter, and more personal.

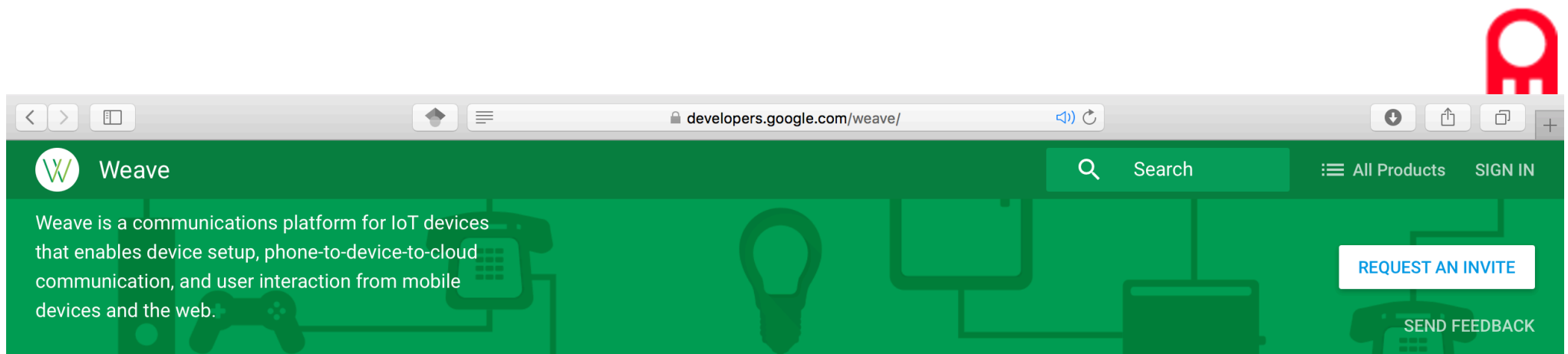We've rebuilt everything for speed and simplicity, so it's easier than ever to tap and go.

WHAT'S NEW

The new ... app is here—and it's all about making your ... experience **faster**, **smarter**, and **more personal**.

We've rebuilt everything for **speed** and **simplicity**, so it's **easier** than ever to tap and go.

Easy device setup   A more connected world   Smart devices

Weave

Search | All Products | SIGN IN

Weave is a communications platform for IoT devices that enables device setup, phone-to-device-to-cloud communication, and user interaction from mobile devices and the web.

REQUEST AN INVITE

SEND FEEDBACK

Easy device setup

Using built-in Weave functionality, you can provide your users with a secure and consistent setup experience that includes automatic install of your mobile app on Android.

A more connected world

Use Weave to connect devices directly or through the cloud. Enable users to interact with their devices through their mobile phone or desktop.

Smart devices

Weave provides a foundation of easy communication for reaching your devices from web or mobile, and standardized schemas that define device interoperability regardless of brand or manufacturer so you can focus on what really matters: creating an

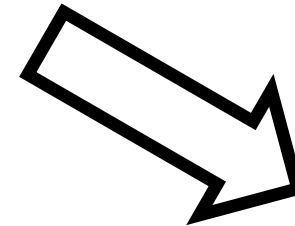G. Alpar (OU), TouW Symposium, 19-11-2016

Web
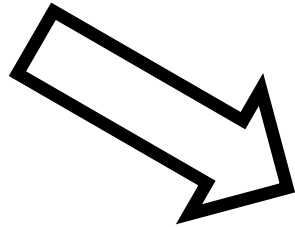
Mobile

IoT

No privacy by current infrastructure

- No possibility of anonymity

  - At best, not default

  - Transactions are based on identification

- Data collection: overwhelming and central   +

  - Always linkable (cookies)
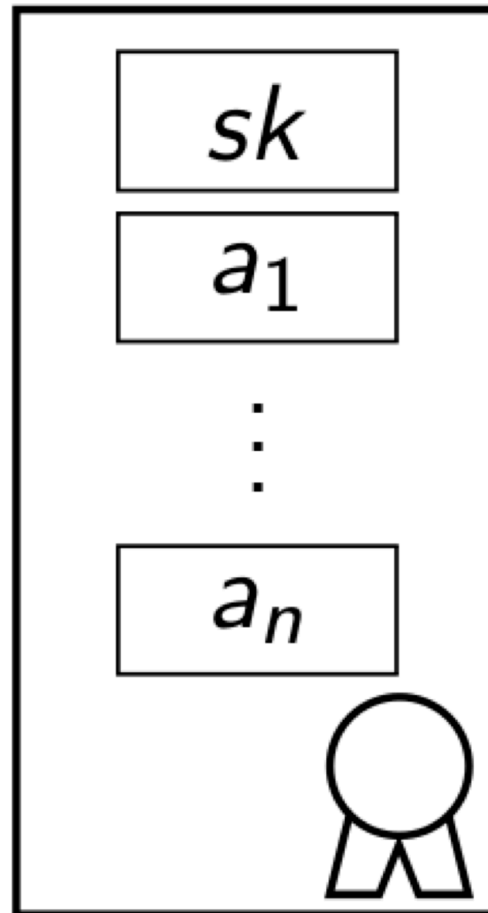
- Data storage and processing: central

Agenda

- IoT and people

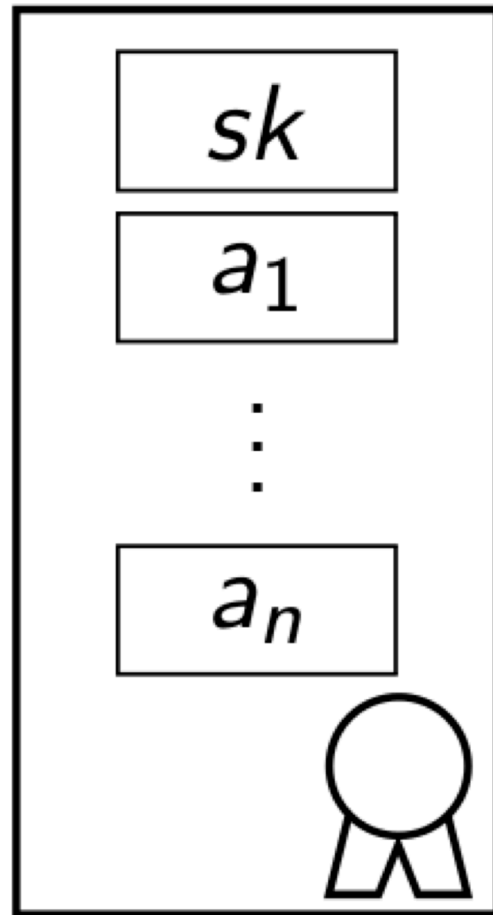- Central and linkable data processing

- **Attributes in IoT**

- Conclusion

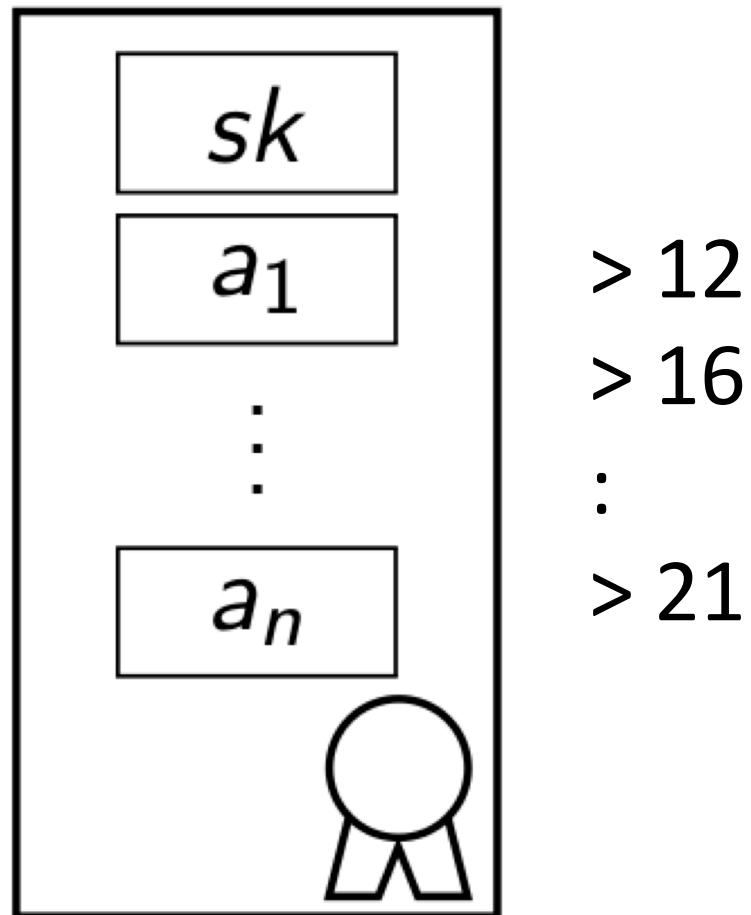# Attribute-based credential

An ABC: citizen identity

sk

a_1

$\vdots$

a_n

citizen identity

Name: G. Alpar
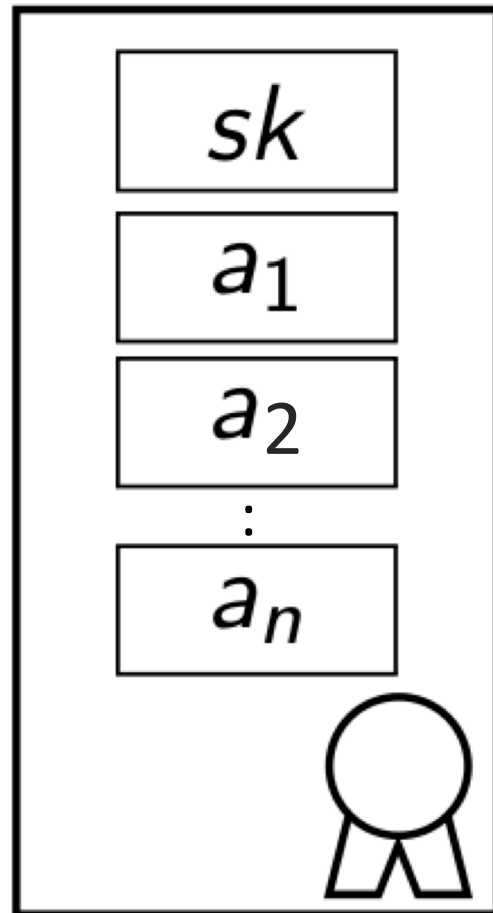
Resident of: Nijmegen

:

BSN: 426538871

An ABC: junior overage

junior overage

> 12
> 16
:
> 21

Authenticating using residence
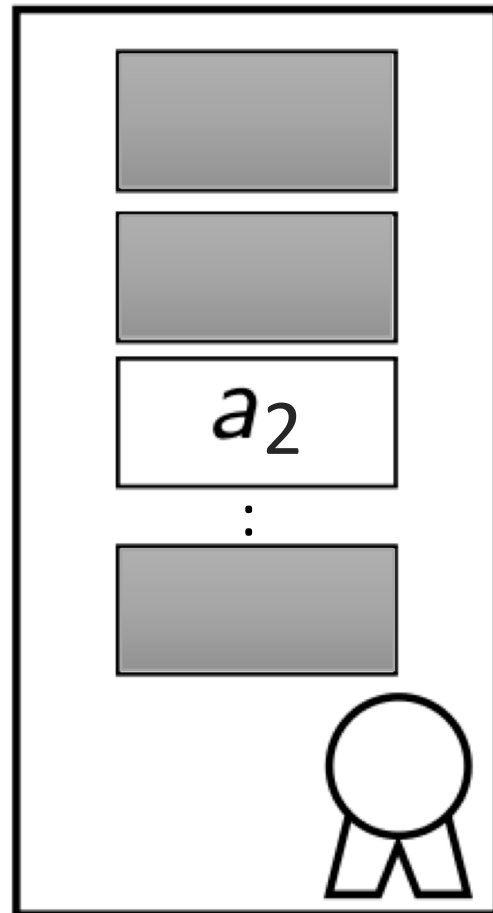

citizen identity

Name: G. Alpar

Resident of: Nijmegen

:

BSN: 426538871

ABC function: selective disclosure

citizen identity
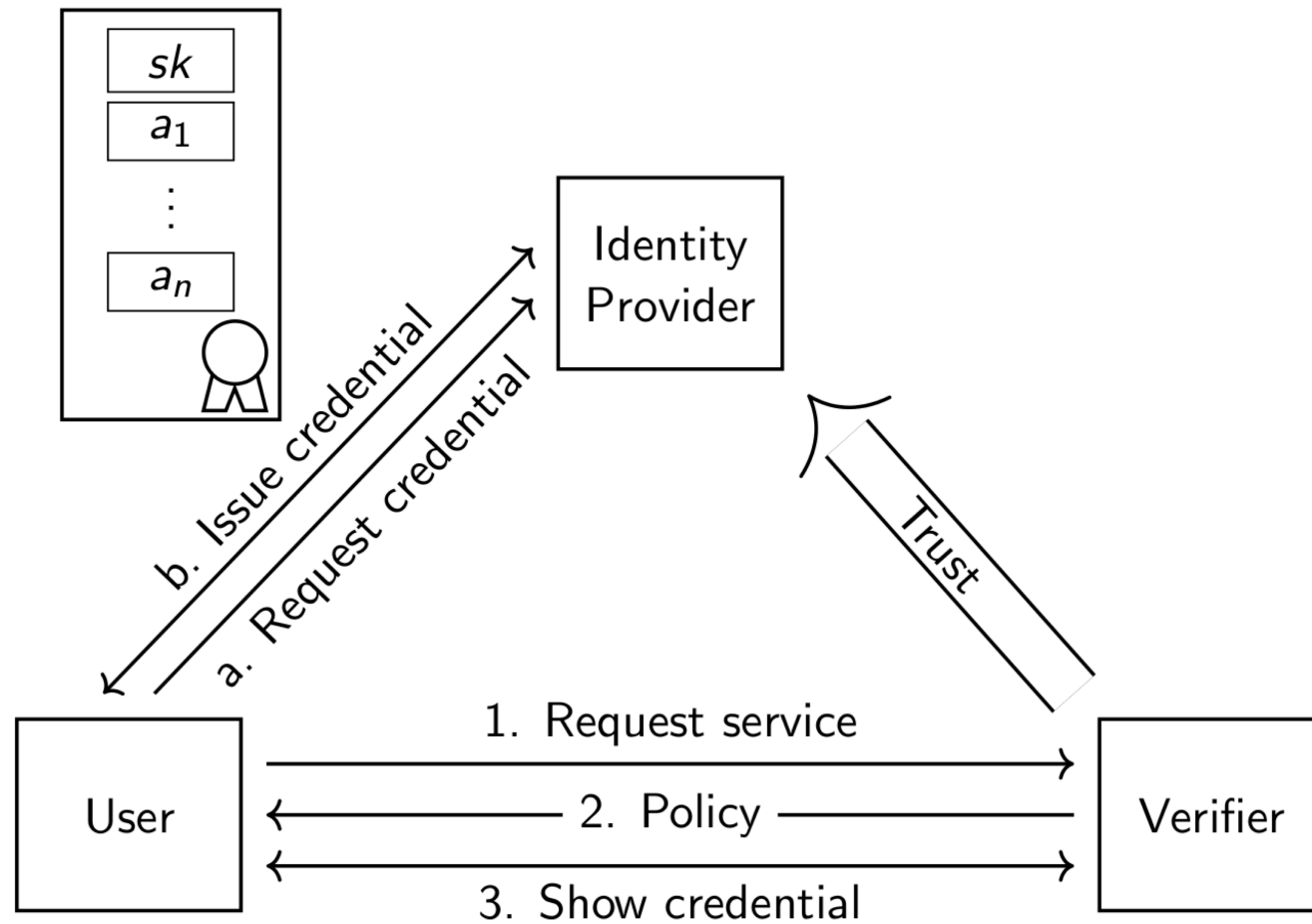
Name: G. Alpar

Resident of: Nijmegen

:

BSN: 426538871

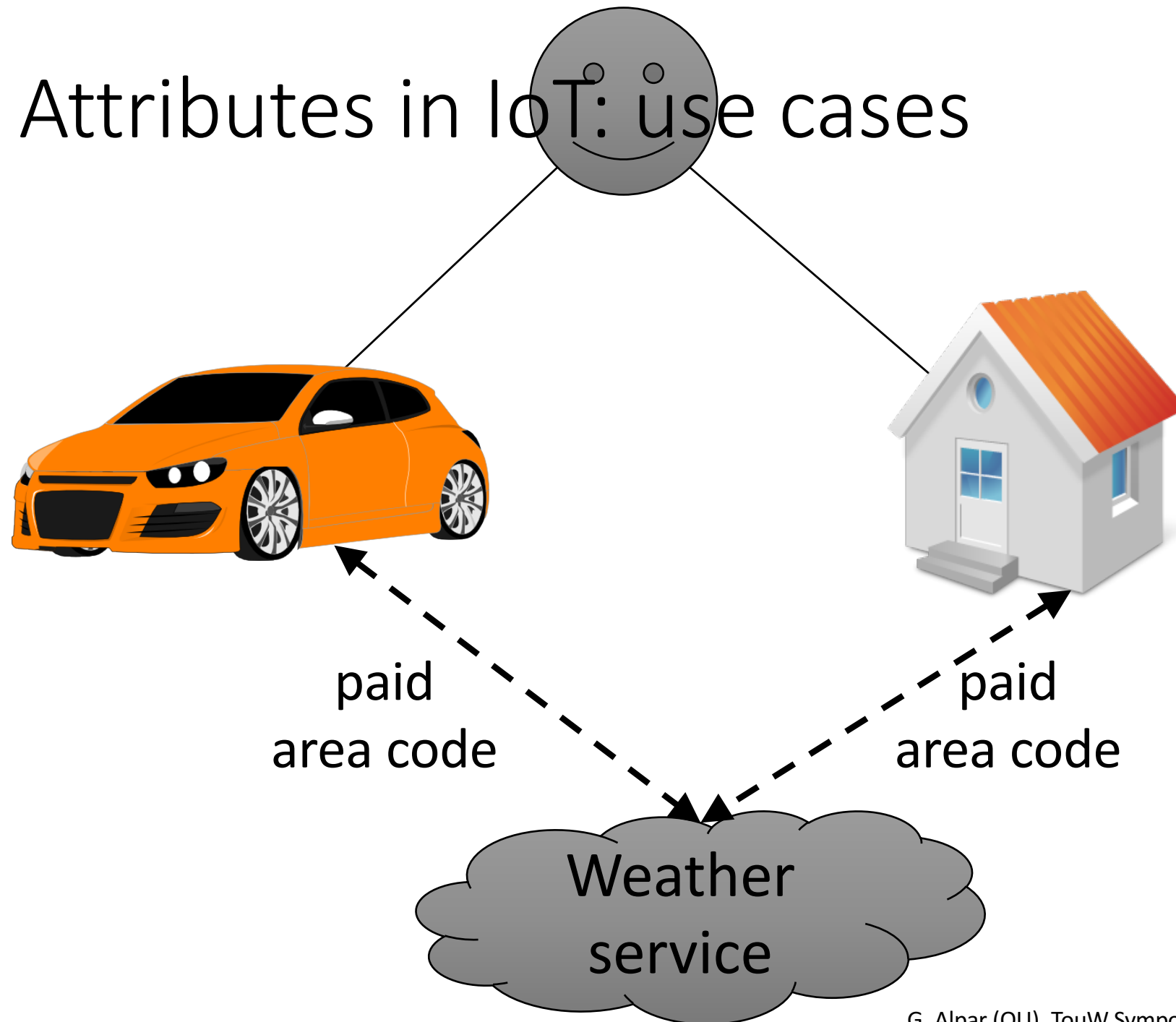# ABC flow

by courtesy of W. Lueks

IRMATube – demo
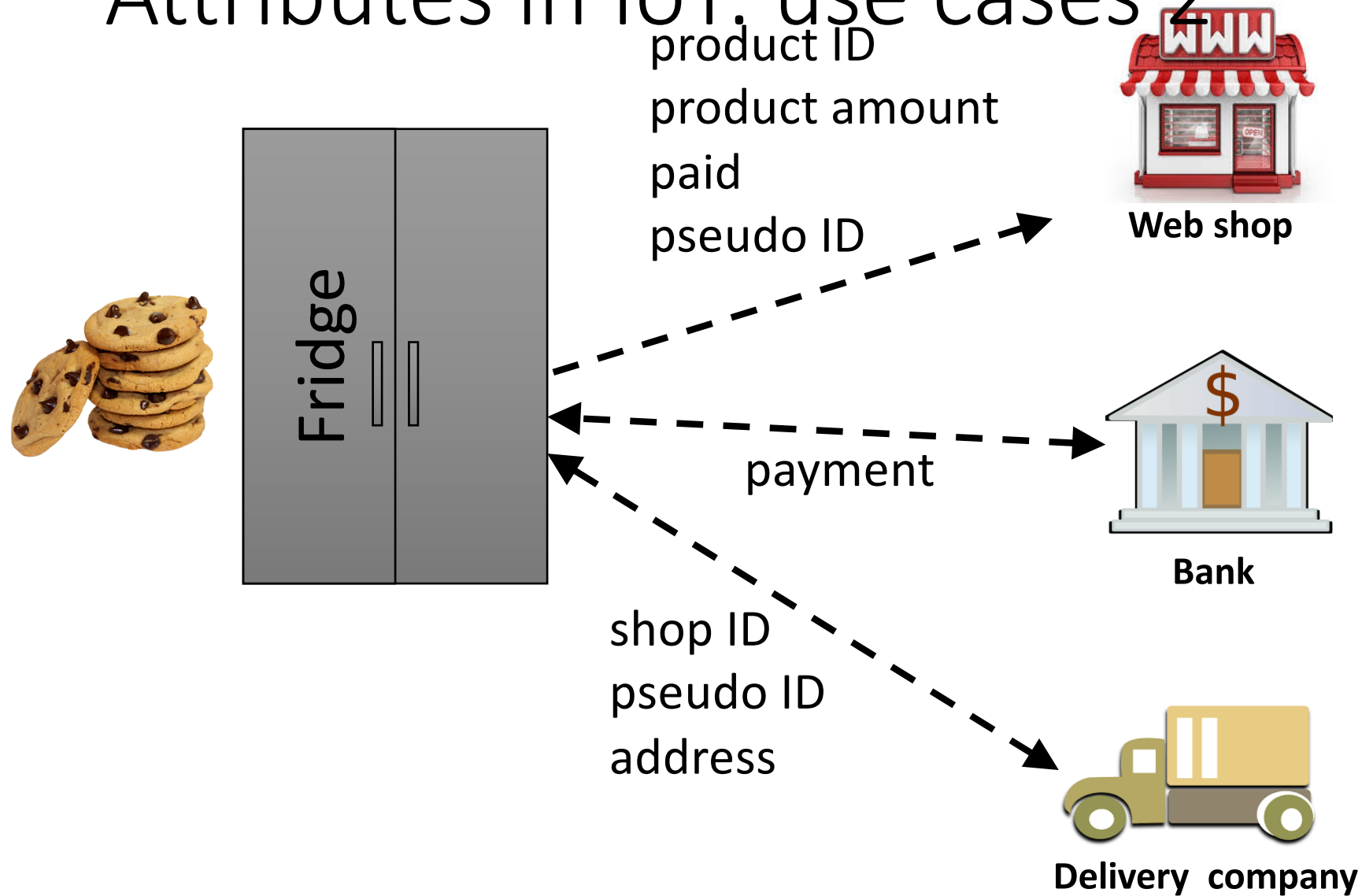

http://demo.irmacard.org // IRMATube

Attributes in IoT: use cases

paid
area code

paid
area code

Weather
service

Attributes in IoT: use cases 2

product ID
product amount
paid
pseudo ID

Web shop

Fridge

payment

Bank

shop ID
pseudo ID
address

Delivery company

Agenda

- IoT and people

- Central and linkable data processing

- Attributes in IoT

- **Conclusion**

Preserving privacy with IoT present

- Possibility of anonymity

- Privacy at data collection: data minimisation

- Decentralisation   +
  - Cryptographic sharing of data (e.g. secret sharing)
  - User-side data storage

- Transactions without identification
  - Attributes instead of identities

- Design with human aspects beyond legal compliance

Discussion

- Web, mobility, IoT and online marketing
  - Privacy, convenience, business – Are they in balance?

- Omitted: Bulk data collection by intelligence services
  - Privacy (democracy), security – Are they in balance?

- Omitted: Data protection and privacy
  - Hacking happens on a daily bases (e.g. zero-day)
  - IoT attacks started

Conclusion

- Smooth transition from Web to IoT with regard to marketing?

- What can you do as a computer scientist, a researcher, a programmer, a software engineer or as a human being to improve on our privacy in our cyber-physical reality?
  - Design, implement and organise with privacy in mind…
  - … not to have too much (third-party) cookies in our fridge!

Thank you!