

# OnLITE: On-line Label for IoT Transparency Enhancement

Alexander Railean and Delphine Reinhardt

# Motivation

- Proliferation of IoT devices
- Privacy impact of data collection
- The GDPR calls for transparency solutions
- This is not a solved problem yet

# Assumptions [about the conference audience]

- You are familiar with IoT
- You are aware of the privacy implications

# Objectives

- Improve IoT transparency as defined by the GDPR
  - **What** data are collected?
  - **Where** are they stored?
  - **How long** are they kept?
  - **For what** purpose are they used?
  - **Who** has access to the data?
- Help *non-experts* understand the impact
- Facilitate comparisons
- Decide at a glance
- Reusable outside IoT (e.g., smartphone apps)

# Means: printed label

- Tested with 31 participants
- Easy to interpret
- Positive feedback
- Published in MobileHCI 2018
- Gaps
  - Who are the partners?
  - What data do they get?
  - What do they use it for?

Hausio T1000

### Privacy facts

<b>Collected data</b>	<b>Sample</b>
customer nr.	
temperature	
humidity	
device Internet address	

**Sent hourly to**  
Tesami GmbH

**Stored for 3 years**  
in France

**All data accessed by**

- You
- Tesami GmbH
- partners

**Purpose of collection**

- your personal use
- scientific research
- targeted advertisements
- product improvement

**Received data**  
Software updates



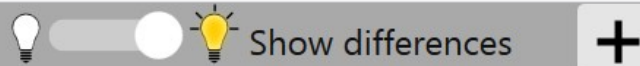
[www.privacy-facts.eu/43dy-kf75](http://www.privacy-facts.eu/43dy-kf75)

# Means: online interface

- Cross-disciplinary design (legal, usability, security, privacy)
- Iterative approach
- Heuristic evaluation with experts
  
- Technical aspects
  - HTML, Javascript, CSS, Python
  - vector graphics with SVG
  - accessibility, semantic markup

# Means: online interface

- Cross-disciplinary design (legal, usability, security, privacy)
- Iterative approach
- Heuristic evaluation with experts
- Technical aspects
  - HTML, Javascript, CSS, Python
  - vector graphics with SVG
  - accessibility, semantic markup
- Design principles
  - tabular format
  - progressive disclosure
  - use bullet-points
  - simple terminology
  - avoid sentences
  - channel redundancy (text, graphic)
  - classic UI widgets
  - “Intelligence amplified”



Show differences



Hausio T1000 ▾

vs

Casami FX ▾

Domowoj ▾

**Collected data**

👤 customer nr.

🌡 temperature

💧 humidity

🌐 device Internet address

👤 customer nr.

🌡 temperature

💧 humidity

🌀 wind speed

👤 customer nr.

🌡 temperature

☀ UV radiation

🌀 wind speed

**Sent**

hourly

to Tesami GmbH

daily

to Aster SRL

daily

to Domotics s.r.o.

## See who gets the data, and why

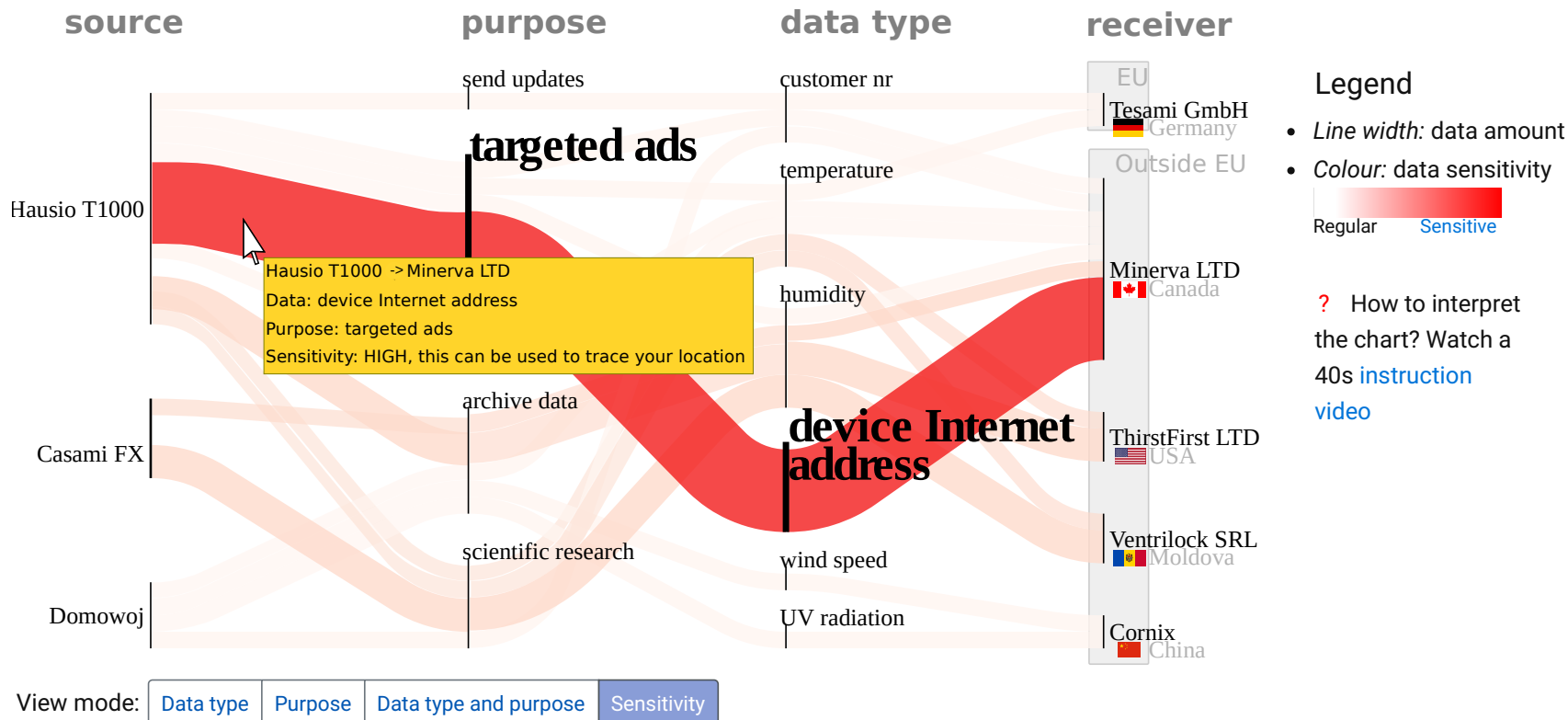
Search in table: 

Device	↕	Data type	↕	Purpose	↕	Company	↕	Country	↕	Sensitivity	↕
Casami FX		🌡 temperature		scientific research		Minerva LTD		🇨🇦 Canada		low	
Casami FX		💧 humidity		scientific research		Minerva LTD		🇨🇦 Canada		low	
Domowoj		☀ UV radiation		archive data		Cornix		🇨🇳 China		low	
Domowoj		👤 customer nr.		scientific research		Minerva LTD		🇨🇦 Canada		low	
Hausio T1000		👤 customer nr.		targeted ads		Minerva LTD		🇨🇦 Canada		low	
Hausio T1000		🌡 temperature		targeted ads		Minerva LTD		🇨🇦 Canada		low	
Hausio T1000		💧 humidity		targeted ads		ThirstFirst LTD		🇺🇸 USA		low	
Hausio T1000		💧 humidity		archive data		Minerva LTD		🇨🇦 Canada		low	
Hausio T1000		🌐 device Internet address		targeted ads		Minerva LTD		🇨🇦 Canada		⚠ high	

Showing 1 to 9 of 9 entries (filtered from 17 total entries)









Follow the flows to see how data are shared with other companies



[Overview](#)[Who gets the data](#)[Data flows](#)[Data sample](#)[Security](#)[Lifecycle](#)[Contact](#)

This table shows actual samples of data collected by each device

Data	Hausio T1000	Casami FX	Domowoj
 customer nr.	481-AHR-1831	mustermann@kiel.de	+43-517987-891
 temperature	22 °C	22 °C	22 °C
 humidity	34%	34%	-
 UV index	-	-	moderate
 wind speed	-	2 m/s	2 m/s
 device Internet address	93.184.216.34	-	-

	Hausio T1000	Casami FX	Domowoj
<b>Vulnerabilities</b>			
Reaction time to disclosed vulnerabilities	2 weeks	3 weeks	-
Rewards for reported vulnerabilities	Yes	Yes	No
<b>Communications</b>			
Secure from Internet eavesdroppers	Yes	-	-
Secure from local network eavesdroppers	Yes	Yes	No
<b>Storage</b>			
Stored data are encrypted	N/A, no information is stored on the device	Yes	No

Protected in a way that makes the data unreadable to persons who do not have the password

More technical details...

- Hausio T1000**
- TLS 1.2 with mutual authentication is used when transmitting the data to the server;
  - The cipher suite is TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA;
  - The private key is generated by and stored inside a secure enclave, ATECC-608A;
  - No information is stored locally.

- Casami FX**
- Military-grade security is applied to ensure your data are safe.

- Domowoj**
- Transmitted data are encrypted with AES-256 in CBC-mode;
  - Locally stored data are not encrypted.

Features grouped by phases of the device lifetime: set-up → usage → maintenance → retiring

	Hausio T1000	Casami FX	Domowoj
<b>Set up</b> – <i>preparing the device for use</i>			
Unique factory-set password	Yes	Yes	No
Password change required before remote access for the first time	Yes	No	No
<b>Use</b> – <i>typical, daily interactions with the device</i>			
Multiple user accounts	Supported	Supported	No
Separate accounts for children	Supported	Supported	No
Separate account for guests	Supported	No	No
<b>Maintenance</b> – <i>procedures to increase the device longevity and ensure it works well</i>			
Automatic updates	Yes	Yes	No
Manual approval of updates	Optional	No	No
Update availability indication	In smartphone app	Mailing list	No
Feature update period	August 2020	August 2019	December 2020
Security update period	December 2023	August 2019	December 2020
Long-term support	January 2024 <a href="#">source code release</a>	-	-
<b>Retiring</b> – <i>when the device is sold, sent for repairs, donated or thrown away</i>			
Secure data deletion (wiping)	Yes	No	No

Action	Hausio T1000	Casami FX	Domowoj
View, edit or delete collected data by contacting the <i>Data Controller</i>	Tesami GmbH Flachmatuchstr. 42, Kiel, 24148, Germany. info@tesa.mi	Aster SRL Via Macaroni 113, Verona, Italy. contact@casam.it	Domotics s.r.o Bezručova 202, Brno, Czech Republic. gosti@dom.cz
Report privacy-related issues to the <i>Data Protection Officer</i>	dpo@tesa.mi	info@casam.it	rucitel@dom.cz
Lodge a complaint with the <i>supervisory authority</i>	<i>Unabhängiges Landeszentrum für Datenschutz</i> Holstenstraße 98, 24103 Kiel, Germany. mail@datenschutzzentrum.de	<i>Garante per la protezione dei dati personali</i> Piazza di Monte Citorio, Roma, Italy.	<i>Orgánem pro ochranu údajů</i> Svoboda 900, Praha, Czech Republic. pomoc@opou.cz

You can also lodge a complaint with a [supervisory authority in your area](#).

# Evaluation

- 14 think-aloud tasks, e.g.
  - which company gets most data?
  - what data are used for targeted ads?
  - what data goes outside the EU?
- 8 open-ended questions, e.g.
  - which tab was most helpful?
  - what parts of the UI were not clear?
- SUS questionnaire
  - quantity usability
- Thematic analysis
  - typical friction points
  - common usage patterns

# Evaluation

- 15 participants
- 10 EUR (opt out)
- Conducted in Kiel, Germany

Backgrounds: economists,  
mathematicians, computer scientists,  
environmentalists, and lawyers

Countries: Brazil, Peru, Mexico, Spain,  
Germany, Moldova, China, Vietnam,  
India, Pakistan, Iran, Ghana

	<b>Age</b>	<b>Sex</b>	<b>Skill</b>
P1	27..35	F	expert
P2	27..35	M	expert
P3	18..26	F	expert
P4	27..35	F	interm.
P5	27..35	F	interm.
P6	36..44	M	expert
P7	18..26	M	novice
P8	27..35	F	interm.
P9	18..26	F	expert
P10	27..35	M	expert
P11	27..35	-	expert
P12	36..44	M	expert
P13	27..35	M	expert
P14	27..35	M	interm.
P15	27..35	M	novice

# Results

- Covers the gaps of the printed version
- Qualitative feedback is very positive
- Participants found OnLITE helpful
- ... and would like to have such a UI in reality
- The tabular layout works well
- Graphical flows (Sankey diagrams)
  - Some like them more
  - It may take a while to understand them
- Interactivity makes interpretation easier
- “Overview” is most informative tab, followed by “Who gets the data” and “Flows“



## Selected themes and quotes

- OnLITE encourages **critical thinking**, e.g.,
  - “6 years, that’s a long time for such a small purpose, I can’t say it is reasonable” (P15)
  - “Truth be told, I don’t understand why they need to store the device Internet address” (P2)
  - “Why would a temperature measuring device have this feature? This I don’t understand” (P11)
- Participants would trust the information if it were **vetted by a reputable organization**:
  - “I will trust the EU” (P15)
  - “Anything related to the government” (P6)
  - But they *failed to name a specific organization!*
- Participants think OnLITE is **complete**:
  - “... it looks very complete” (P6)
  - “... there’s nothing else I could add that comes to mind” (P8)

## Selected themes and quotes

- OnLITE provides an **educational opportunity**, e.g.,  
“I won't be very stressed or concerned if the information about the temperature in my apartment, for example, would be read by someone else. *I mean, what can they do? I'm just... I'm guessing*” (P2)

device  
Internet address

device Internet address → Minerva LTD

HIGH sensitivity

This can be used to trace your physical location

“The highlighting is really cool!” (P1)

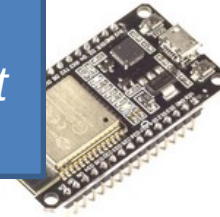


Hausio T1000 ▾

VS Casami FX ▾

Domowoj ▾

“[This tab] gives information about what parameters are collected and also how long this info is stored. *It is the most helpful.* If you want more details, you go to other tabs” (P2)



### Collected data

customer nr.

temperature

humidity

device Internet address

customer nr.

temperature

humidity

wind speed

customer nr.

temperature

UV radiation

wind speed

### Sent

hourly

to Tesami GmbH

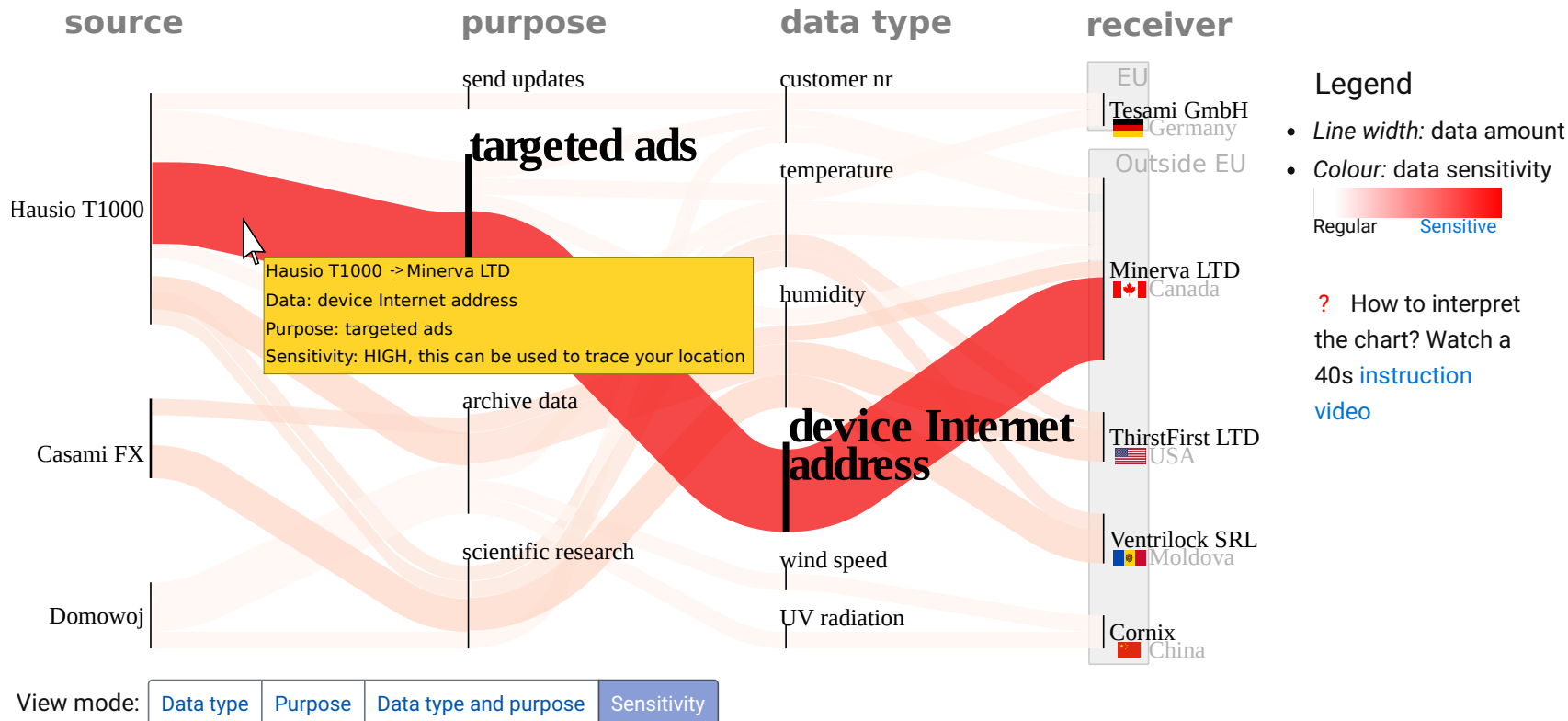
daily

to Aster SRL

daily

to Domotics s.r.o.

“The *faster* way for me was looking at the data flow, it was more *concise!*” (P12)  
 “... same information as in the table, but shown in a graphical way, *very beautiful!*” (P2)



## Which customer number is more privacy-preserving?

“I think the first one is better, because it is just a sequence of numbers and letters” (P1)

“The first one for sure!” (P6)

[Overview](#)

[Who gets the data](#)

[Data flows](#)







[Data sample](#)

[Security](#)

[Lifecycle](#)

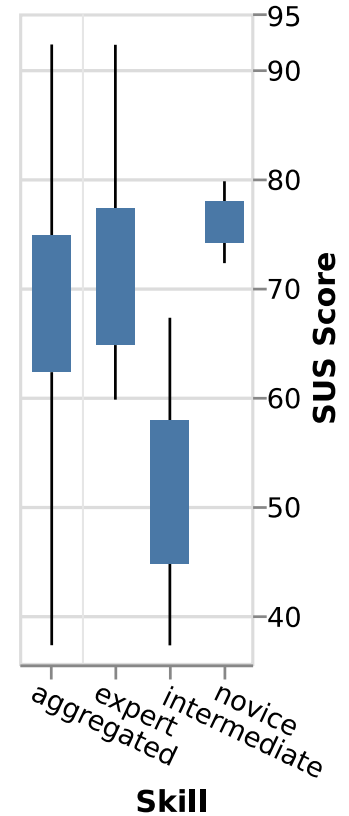
[Contact](#)

This table shows actual samples of data collected by each device

Data	Hausio T1000	Casami FX	Domowoj
 customer nr.	481-AHR-1831	mustermann@kiel.de	+43-517987-891
 temperature	22 °C	22 °C	22 °C
 humidity	34%	34%	-
 UV index	-	-	moderate
 wind speed	-	2 m/s	2 m/s
 device Internet address	93.184.216.34	-	-

## SUS Time (minutes)

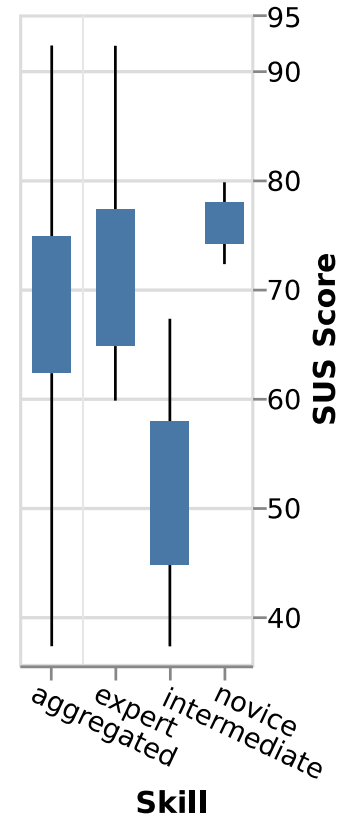
	Age	Sex	Skill	score	Tasks	Interv.	Total
P1	27..35	F	expert	92.5	40	13	53
P2	27..35	M	expert	90	43	24	67
P3	18..26	F	expert	60	40	16	56
P4	27..35	F	interm.	67.5	42	15	57
P5	27..35	F	interm.	55	36	19	55
P6	36..44	M	expert	72.5	39	15	54
P7	18..26	M	novice	80	30	12	42
P8	27..35	F	interm.	37.5	42	18	60
P9	18..26	F	expert	65	39	25	64
P10	27..35	M	expert	70	49	11	60
P11	27..35	-	expert	77.5	55	21	76
P12	36..44	M	expert	67.5	27	26	53
P13	27..35	M	expert	65	47	12	59
P14	27..35	M	interm.	47.5	38	20	58
P15	27..35	M	novice	72.5	28	23	51



The mean score matches the industry mean of 68.

- contrast with the qualitative data
- no other scores to compare with yet

P1	27..35	F	expert	92.5	40	13	53
P2	27..35	M	expert	90	43	24	67
P3	18..26	F	expert	60	40	16	56
P4	27..35	F	interm.	67.5	42	15	57
P5	27..35	F	interm.	55	36	19	55
<hr/>							
P6	36..44	M	expert	72.5	39	15	54
P7	18..26	M	novice	80	30	12	42
P8	27..35	F	interm.	37.5	42	18	60
P9	18..26	F	expert	65	39	25	64
P10	27..35	M	expert	70	49	11	60
<hr/>							
P11	27..35	-	expert	77.5	55	21	76
P12	36..44	M	expert	67.5	27	26	53
P13	27..35	M	expert	65	47	12	59
P14	27..35	M	interm.	47.5	38	20	58
P15	27..35	M	novice	72.5	28	23	51



The mean score matches the industry mean of 68.

- contrast with the qualitative data
- no other scores to compare with yet

P1	27..35	F	expert	92.5	40	13	53
----	--------	---	--------	------	----	----	----

P2	27..35	M	expert	90	43	24	67
----	--------	---	--------	----	----	----	----

No significant difference between the SUS scores of

- experts and non-experts
- age groups
- gender groups

P7	18..26	M	novice	80	50	12	42
----	--------	---	--------	----	----	----	----

P8	27..35	F	interm.	37.5	42	18	60
----	--------	---	---------	------	----	----	----

P9	18..26	F	expert	65	39	25	64
----	--------	---	--------	----	----	----	----

P10	27..35	M	expert	70	49	11	60
-----	--------	---	--------	----	----	----	----

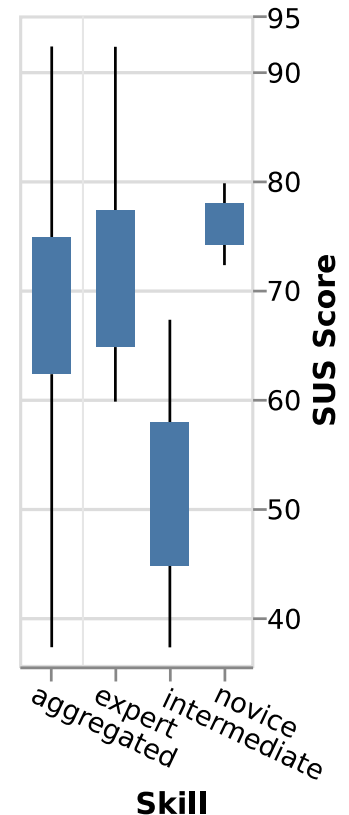
P11	27..35	-	expert	77.5	55	21	76
-----	--------	---	--------	------	----	----	----

P12	36..44	M	expert	67.5	27	26	53
-----	--------	---	--------	------	----	----	----

P13	27..35	M	expert	65	47	12	59
-----	--------	---	--------	----	----	----	----

P14	27..35	M	interm.	47.5	38	20	58
-----	--------	---	---------	------	----	----	----

P15	27..35	M	novice	72.5	28	23	51
-----	--------	---	--------	------	----	----	----





# Summary of our contribution

- GDPR-centric transparency interface for IoT
- User-validated UI
- Laconic visualization of large data-sets
- Shared SUS scores for comparisons with alternatives
- Source-code for replication and derivative works

# Call to action

- Try it: **privacy-facts.eu**
- *Tinker* with the source code
- Provide *feedback*
  - weaknesses
  - improvements
  - new use cases
- Talk to your *friends* about it
- Mention it to *policy-makers*

## Call to action

- Try it: [privacy-facts.eu](https://privacy-facts.eu)
- *Tinker* with the source code
- Provide *feedback*
  - weaknesses
  - improvements
  - new use cases
- Talk to your *friends* about it
- Mention it to *policy-makers*

## Thanks to

- Heuristic evaluators
- Participants
- Privacy&Us
- ULD (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)
- USECON
- Open source community

[arailea@cs.uni-goettingen.de](mailto:arailea@cs.uni-goettingen.de)

This research has received funding from the H2020 Marie Skłodowska-Curie EU project "Privacy&Us" under the grant agreement No 675730.

# Bonus slides

- You've unlocked a secret area!

# Replication bundle

- Check **privacy-facts.eu** to find
  - more screenshots
  - source code and instructions
  - statistical calculations
  - other supplementary materials

## Other remarks

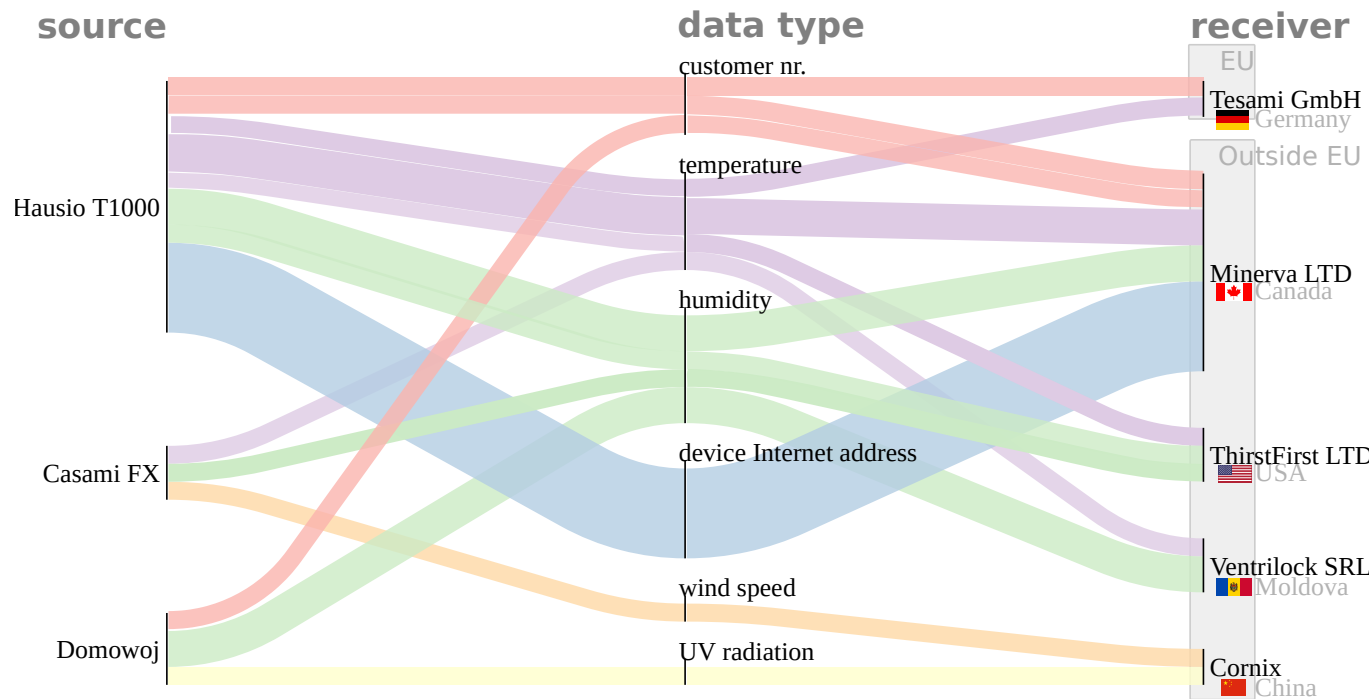
- „Military-grade security“ was planted in the “more technical details” section of “Security” (on slide#11) to see whether participants would want to clarify what it means.
  - Nobody did
  - We do not endorse the use of such terms

# How the level of expertise was evaluated

- Novice < 8 < intermediate < 20 < expert

<b>Points</b>	<b>Skills</b>
2	play video games
2	view photos and watch videos
2	browse the Internet and send emails
2	use a word-processor to type documents
5	set up email sorting filters
5	type complex documents in word processors (e.g. macros, automatic indexes, dynamic fields)
10	assemble computers or other electronics from components
15	I know at least one programming language

Follow the flows to see how data are shared with other companies



### Legend

- *Line width:* data amount
- *Colour:* type of collected data

How to interpret the chart? Watch a 40s [instruction video](#)

View mode: [Data type](#) [Purpose](#) [Data type and purpose](#) [Sensitivity](#)



### Privacy facts

**Collected data**  
 👤 customer nr.  
 🌡️ temperature  
 💧 humidity  
 🌐 device Internet address

**Sample**



QR contents

**Sent hourly to**  
Tesami GmbH

**Stored for 3 years**  
in France

**All data accessed by**

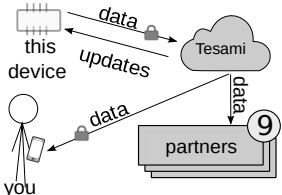
- You
- Tesami GmbH
- partners

**Purpose of collection**

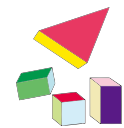
- your personal use
- scientific research
- targeted advertisements
- product improvement

**Received data**

Software updates



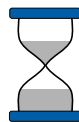
[www.privacy-facts.eu/43dy-kf75](http://www.privacy-facts.eu/43dy-kf75)



## What?



## Where?



## How long?



## Who?



## Purpose?

customer number = 481-AHR-1831  
 temperature = 22 C  
 humidity = 34%  
 device Internet address = 93.184.216.34

URL to OnLITE

That's all, fellow scholars!