Improving the Transparency of Privacy Terms Updates

Opinion paper

Alexander Railean and Delphine Reinhardt

Motivation

- Lengthy privacy terms
- Complicated language, vagueness
- Updated terms are lengthy too
- Fatigue
- The GDPR calls for transparency solutions

Schaub et al., “A Design Space for Effective Privacy Notices”
McDonald et al., “The Cost of Reading Privacy Policies”
Okoyomon et al., “On The Ridiculousness of Notice and Consent”

When paper authors compare versions

```
- The table in Fig.~\ref{fig:consent-table} was
  originally conceived as a component of an Online
  Interface for IoT Transparency Enhancement
  (OnLITE), which summarizes privacy facts, and
  makes it easy to compare different IoT devices
  side by side, as shown in Fig.~\ref{fig:onlite-
  diff} \cite{railean_onlite_2020}
```

```
+ The table in Fig.~\ref{fig:consent-table} was
  originally conceived as a component of an Online
  Interface for IoT Transparency Enhancement
  (OnLITE), which summarizes data collection
  practices and privacy information, and makes it
  easy to compare different IoT devices side by
  side, as shown in Fig.~\ref{fig:onlite-diff}
  \cite{railean_onlite_2020}
```

When programmers compare versions

```
@@ -36,6 +36,9 @@ class MqttClient:
     def on_request(self, client, userdata, msg):
         """Invoked when a message is received on t_requests"""
         if self.external_handler:
-            self.external_handler(client, userdata, msg)
+            try:
+                self.external_handler(client, userdata, msg)
+            except Exception as err:
+                log.exception('ERR %err %s %s', err, msg.topic, msg.payload)
         else:
             log.debug("MQTT IN %s %s", msg.topic, msg.payload)
```

When users compare versions…

Image credit: Where’s Wally?

Issues with the status quo

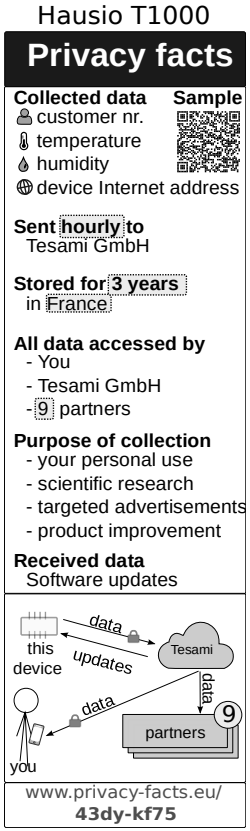
- Not even a side by side comparison
- Can the „summary of changes“ be trusted?
- Normalization of deviance

Objectives

- Make before/after comparisons easier
- Reduce the number of update prompts
- Reduce volume of displayed information
- Standardize representation

Roots: printed label for IoT devices

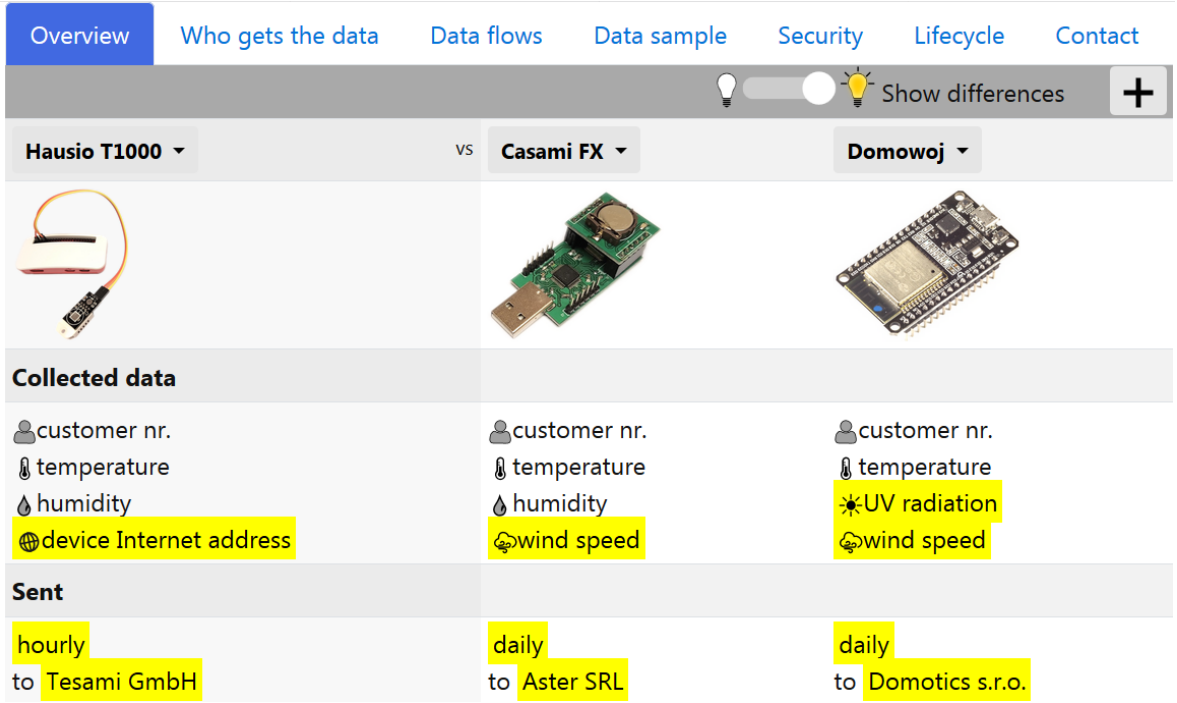
- Tested with 31 participants
- Easy to interpret
- Positive feedback
- Published at MobileHCI 2018 [1]



[1] Railean and Reinhardt, Let there be LITE: design and evaluation of a label for IoT transparency enhancement. http://doi.org/10.1145/3236112.3236126

Roots: online interface

- Cross-disciplinary design(legal, usability, security, privacy)
- Iterative approach
- Heuristic evaluation with experts
- Tested with 15 participants
- Task analysis, interview
- Published at NordSec 2020 [1]



[1] Railean and Reinhardt, OnLITE: On-line Label for IoT Transparency Enhancement https://doi.org/10.1007/978-3-030-70852-8_14

Comparing updated privacy terms

- Compare a device against itself
- Generalize: IoT devices → any privacy terms

Show differences

Hausio T1000 v1.1	vs	Hausio T1000 v1.2
		
Collected data		
customer nr. temperature humidity device Internet address		customer nr. temperature humidity device Internet address wind speed
Sent		
hourly to Tesami GmbH		daily to Tesami GmbH
Stored for		
3 years in France		6 years in France

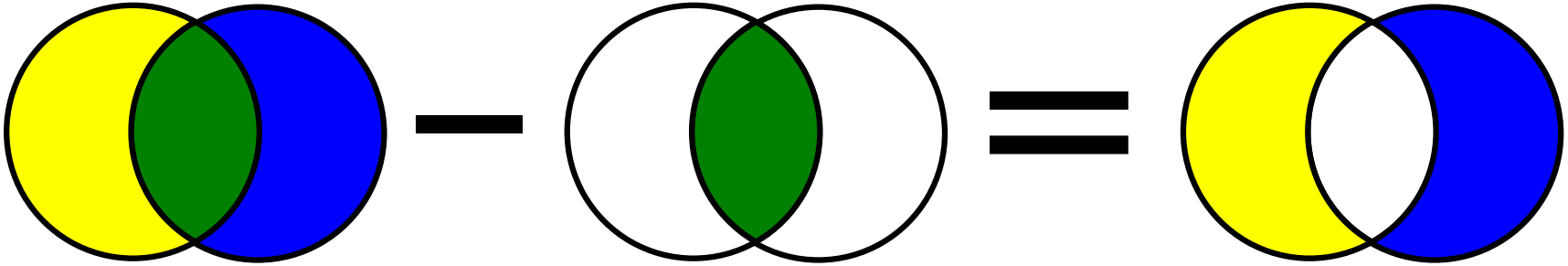
Formal notation of privacy terms

Data type Δ	type of collected data
Purpose Π	purpose of collection
Time T	the retention period
Company C	a company that gets the data
Location Λ	location of said company
Frequency Φ	how often the data are transmitted

Term Θ	a tuple of the form $(\Delta, \Pi, C, \Lambda, T, \Phi)$
Consent K	a set of terms accepted by the user, e.g., $K = \{\Theta_1, \Theta_2, \Theta_3, ..\Theta_i\}$.

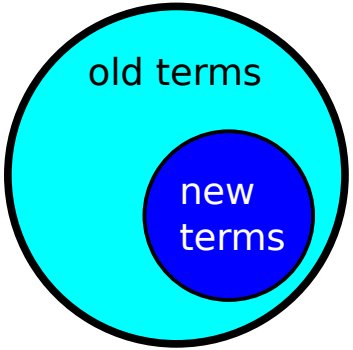
Tuples, tables, and set algebra

Data type ⇅	Purpose ⇅	Company ⇅	Country ⇅	Duration ⇅	Frequency ⇅
🌡 temperature	research	Minerva LTD	🇨🇦 Canada	1y	daily
💧 humidity	marketing	ThirstFirst LTD	🇺🇸 USA	1y	hourly



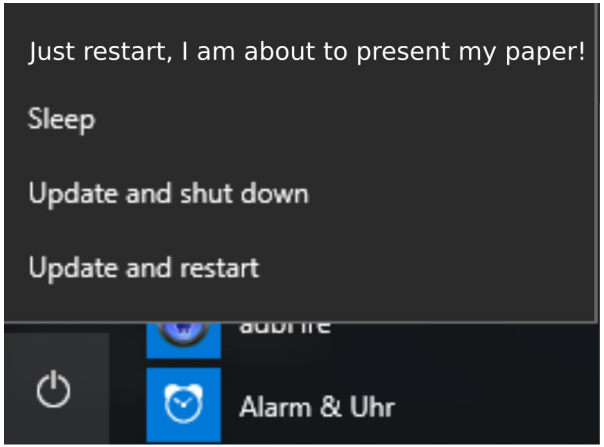
Omitting update prompts

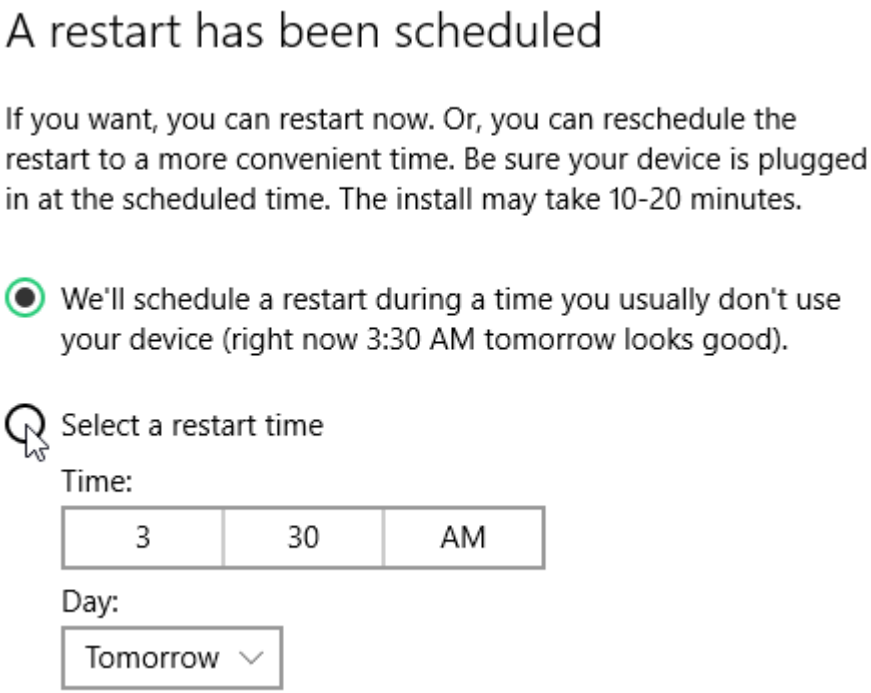
- Formal rules (e.g. new terms are more strict)



Omitting update prompts

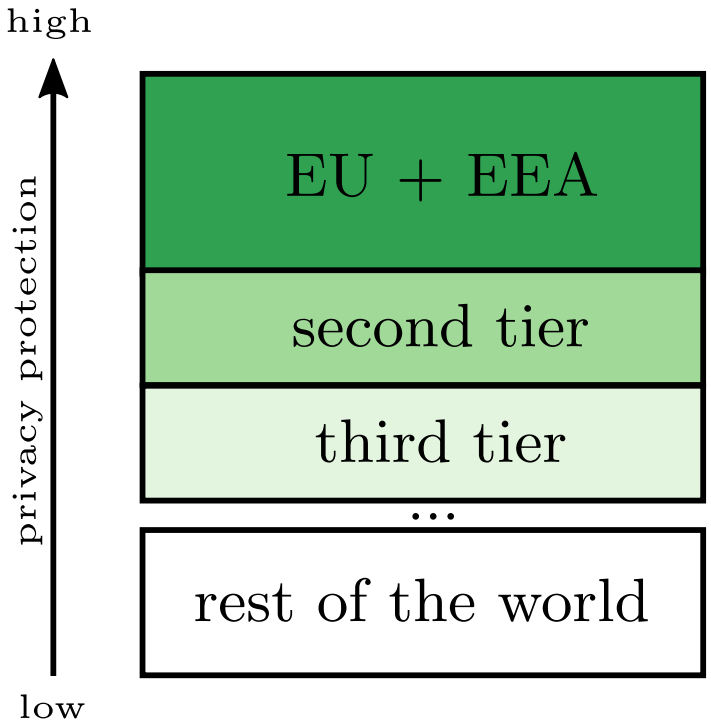
- Formal rules (e.g. new terms are more strict)
- When is the best time to show a prompt?





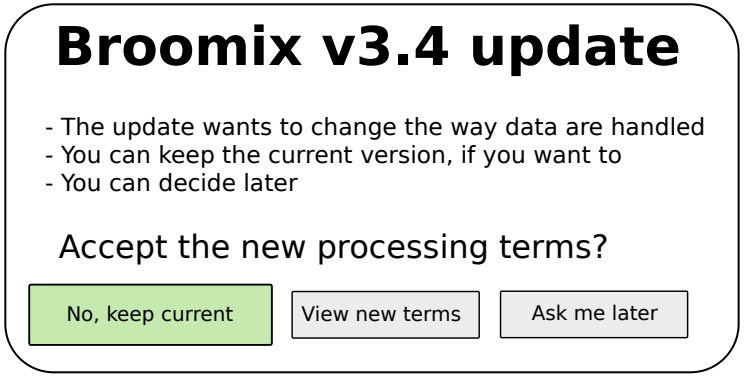
Omitting update prompts

- Formal rules (e.g. new terms are more strict)
- When is the best time to show a prompt?
- Privacy protection gradient



Omitting update prompts

- Formal rules (e.g. new terms are more strict)
- When is the best time to show a prompt?
- Privacy protection gradient
- Decouple feature, security and privacy updates



Reduce information volume

- Inline prompts

Broomix v3.4 update

- The update wants to change the way data are handled
- You can keep the current version, if you want to
- You can decide later

What has changed:

	Data type	Purpose	Company	Country	Duration
new	temperature	research	Minerva LTD	Can	1y
	humidity	marketing	ThirstFirst LTD	USA	~~1y~~ 3y

Accept the new processing terms?

No, keep current | Accept new terms | Ask me later

Reduce information volume

- Inline prompts
- Tabular representation and information efficiency

“We care about your privacy, therefore our smart indoor temperature and humidity meter only collects and shares your data with 2 companies. Temperature data are shared on a daily basis with Minerva LTD, located in Canada. The data are retained for a period of 1 year and are used for research purposes. Humidity is shared on an hourly basis with ThirstFirst LTD, and retained by them for 1 year, in the USA. Humidity data are used for marketing purposes”

Data type ⇅	Purpose ⇅	Company ⇅	Country ⇅	Duration ⇅	Frequency ⇅
🌡 temperature	research	Minerva LTD	🇨🇦 Canada	1y	daily
💧 humidity	marketing	ThirstFirst LTD	🇺🇸 USA	1y	hourly

Other benefits and potential applications

- Granular permissions
- Search engine – e.g., “devices that store *temperature* in *the EU* for *research*“
- Archive of policies
- Privacy assistant

Summary of our contribution

- Formal notation for privacy terms
- Standardized representation of terms
- Information efficiency as a benchmark
- Concrete steps to reduce
  - Effort to compare
  - Volume of displayed information

Call to action

- *Try* our UI: **privacy-facts.eu**
- Provide *feedback*
  - weaknesses
  - improvements
  - new use cases
- Talk to your *friends* about it
- Mention it to *policy-makers*

- Check out our related work
  - Let there be LITE: design and evaluation of a label for IoT transparency enhancement
  - OnLITE: On-line Label for IoT Transparency Enhancement
  - More at s.gwdg.de/ISn2Eg

arailea@cs.uni-goettingen.de

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

Bonus slides

- You‘ve unlocked a secret area!

Image credit: Where’s Wally?

Overview | Who gets the data | Data flows | Data sample | Security | Lifecycle | Contact

“The highlighting is really cool!” (P1)

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.

Hausio T1000

Privacy facts

Collected data **Sample**

- customer nr.
- temperature
- humidity
- device Internet address

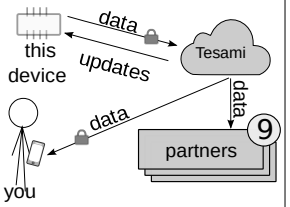
Sent hourly to
Tesami GmbH

Stored for 3 years
in France

All data accessed by
- You
- Tesami GmbH
- 9 partners

Purpose of collection
- your personal use
- scientific research
- targeted advertisements
- product improvement

Received data
Software updates



www.privacy-facts.eu/
43dy-kf75

QR contents

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

URL to OnLITE

What?

Where?

How long?

Who?

Purpose?

Quantifying useful information

	DPV		P3P		Apple	
	items	bits	items	bits	items	bits
Data type	**161**	8	17	5	32	5
Purpose	**31**	5	16	4	6	3
Duration	-	-	**5**	3	-	-

Useful information in a privacy term

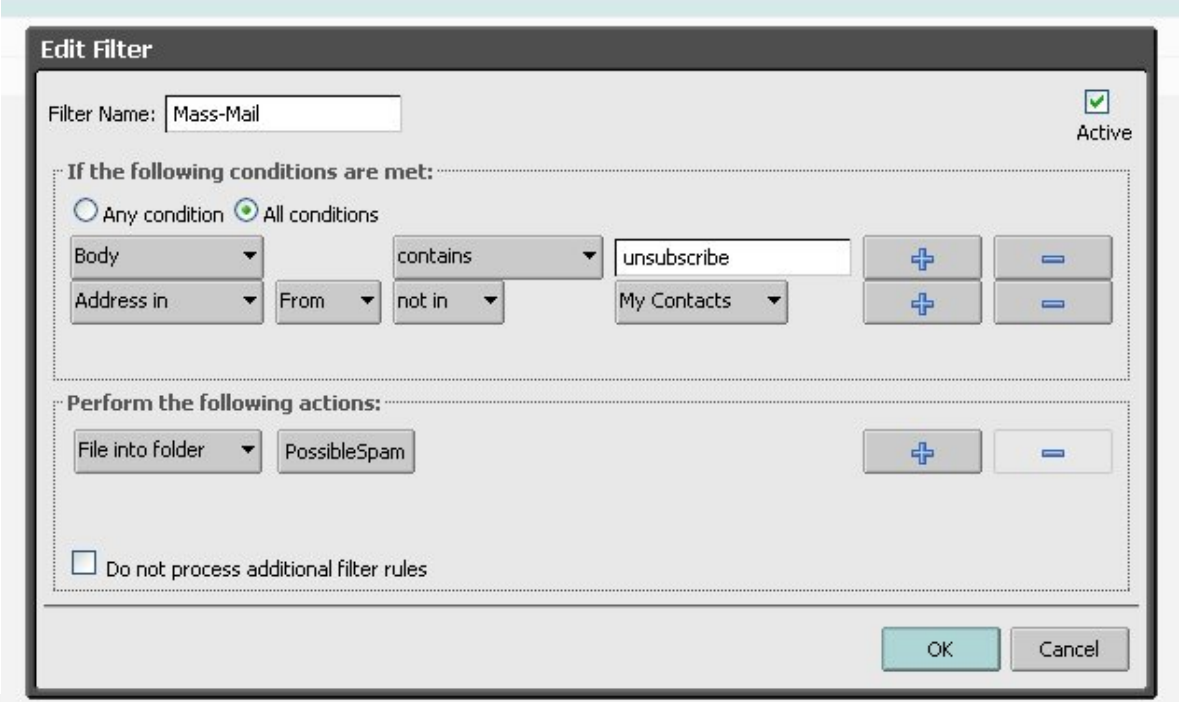
Δ	Π	C	Λ	T	Φ
temperature	research	Minerva LTD	Canada	1 year	daily
161 data types	31 purposes	20 symbols per company 39-symbol alphabet {a..z, 0..9, \t,\n,\space} 6 bit/symbol	193 countries	8 units + n year 0..255 month week day hour minute second	8 frequencies many times per second every second every minute hourly daily weekly monthly on demand
bits **8**	**5**	**20x6=120**	**8**	**3+8=11**	**3**

$\Sigma = \mathit{155}$ bits per privacy term

Encodings, their efficiency and interpretability

- Canada
- CA
- CAN
- The world‘s second-largest country
- 

Privacy rules, like email filters



That‘s all, fellow scholars!