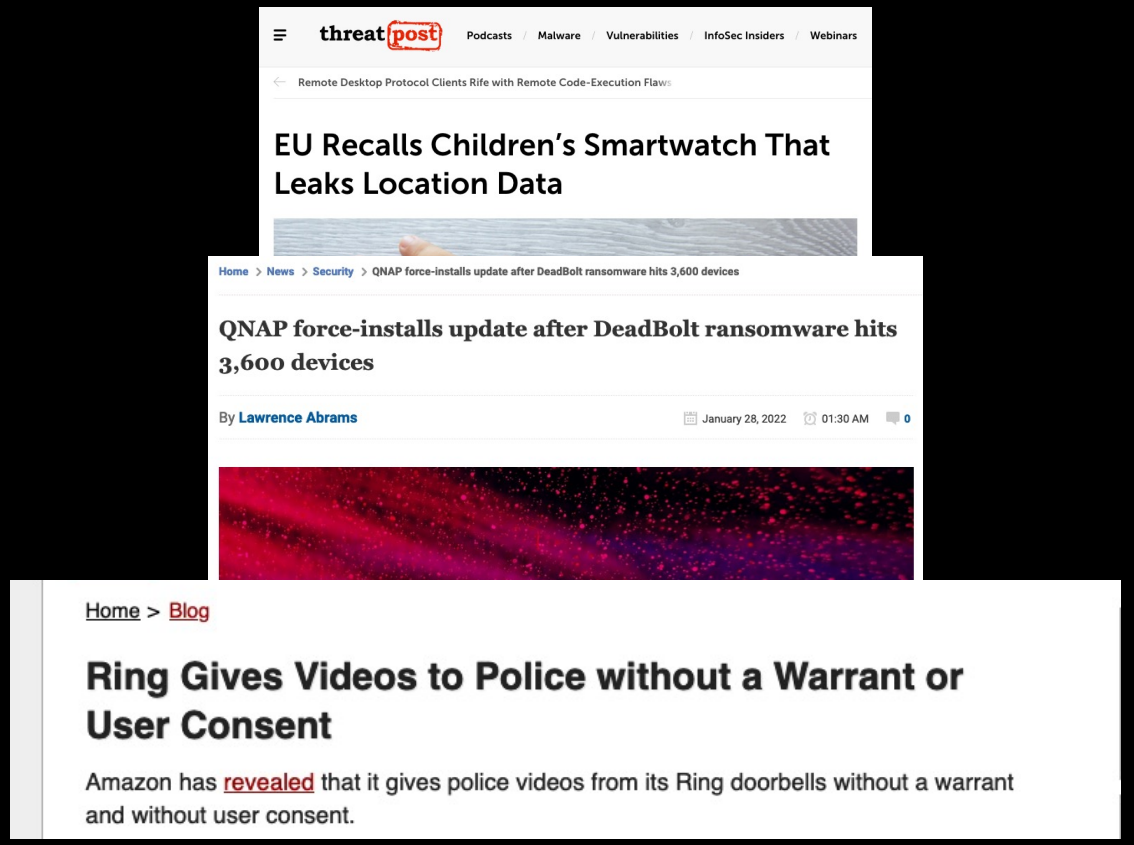
Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible

Lorenz Kustosch*, Carlos Gañán, Mattis van t'Schip,
Michel van Eeten, Simon Parkin

State of IoT Security and Privacy

- IoT security and privacy incidents are still prevalent.
- Inconsistent manufacturer responses.
- Users are often in a poor position to fix their devices.



Consumer Expectations in IoT Security and Privacy

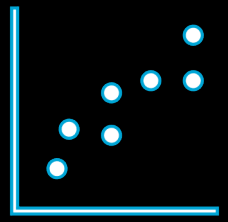
- Which rights and support can users expect when something goes wrong?
- In product liability and conformity law, the concept of "reasonable consumer expectations" can help set a baseline in regulations and court.
- But what is "reasonable" to expect about IoT security and privacy?
- Previous work focused on IoT users' preferences, e.g.,:
  - Desired security measures[1]
  - Appropriate data flows[2]
  - Desired actor responsibilities[3]
- Does not quite capture expectations that are reasonable.

[1] Tabassum, Frik, Malkin, Wijesekera, Egelman, Lipford. *Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants.* (2019)

[2] Abaquita, Bahirat, Badillo-Urquiola, Wisniewski. *Privacy Norms within the Internet of Things Using Contextual Integrity.* (2020)

[3] Haney, Acar, Furman. *"It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security*. (2021)

Motivation: Measuring Expectations



Reasonable

How things are *likely* to be.

Normative

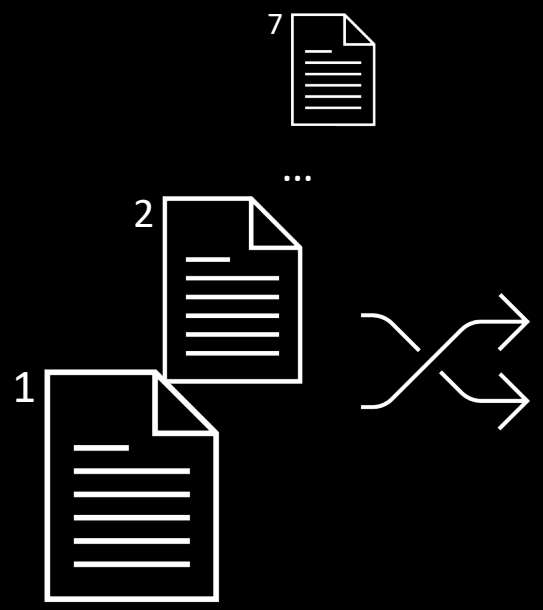
How things *should* be.

Research Questions

- (RQ1) What do consumers expect how manufacturers will respond to emerging privacy and security risks with IoT devices?
- (RQ2) What do consumers expect how manufacturers should respond to emerging privacy and security risks with IoT devices?
- (RQ3) How do participants evaluate the user's responsibility to handle emerging privacy and security risks with IoT devices?

Methodology

- Vignette-driven online survey.
- N = 862, recruited on Prolific.
- Vignette = Fictional text scenario.
- Seven vignettes per participant in random order.
- Based on previous work and news reports.



Example Vignette

Factors:

[1] IoT Device

Alex has several **[1] internet connected security cameras** at home, which are kept switched on continuously. The cameras continually collect video recordings of Alex's home and its surroundings to act as a deterrent against break-ins and allow Alex to check the video feeds remotely from a mobile app via an internet connection.

[2] Security / Privacy Event

Alex reads in a news post that a software vulnerability has been found in this device model and that similar vulnerabilities have been attacked. **[2] The vulnerability could allow other people to remotely install software on the device without Alex noticing**. The device could then be used to remotely attack other websites or devices connected to the internet, but Alex would still be able to use the device without noticing a problem.

[3] Manufacturer Response

In response to this, the **[3] device manufacturer releases a statement on their website** and social media channels, which informs users about the vulnerability and the risks.

[4] User Response

Alex decides to try to **[4] return the devices to the store** where they were bought, hoping to receive a full refund or a replacement

After Each Vignette…

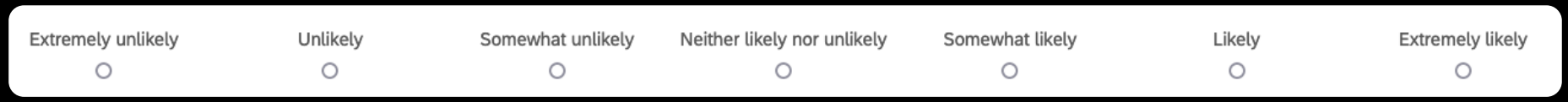
- … respondents were asked if:

  (1) The manufacturer's response was likely.

  (2) The manufacturer's response was appropriate.

  (3) The user's response was suitable to move forward.

- All on a seven point rating scale.



Analysis

1. Vignette factors as categorical predictors...

2. ... to measure effect on expectations via mean responses and regressions.

Factors:

[1] IoT Device

Alex has several **[1] internet connected security cameras** at home, which are kept switched on continuously. The cameras continually collect video recordings of Alex's home and its surroundings to act as a deterrent against break-ins and allow Alex to check the video feeds remotely from a mobile app via an internet connection.

[2] Security / Privacy Event

Alex reads in a news post that a software vulnerability has been found in this device model and that similar vulnerabilities have been attacked. **[2] The vulnerability could allow other people to remotely install software on the device without Alex noticing**. The device could then be used to remotely attack other websites or devices connected to the internet, but Alex would still be able to use the device without noticing a problem.

[3] Manufacturer Response

In response to this, the **[3] device manufacturer releases a statement on their website** and social media channels, which informs users about the vulnerability and the risks.

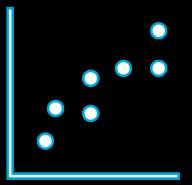
[4] User Response

Alex decides to try to **[4] return the devices to the store** where they were bought, hoping to receive a full refund or a replacement

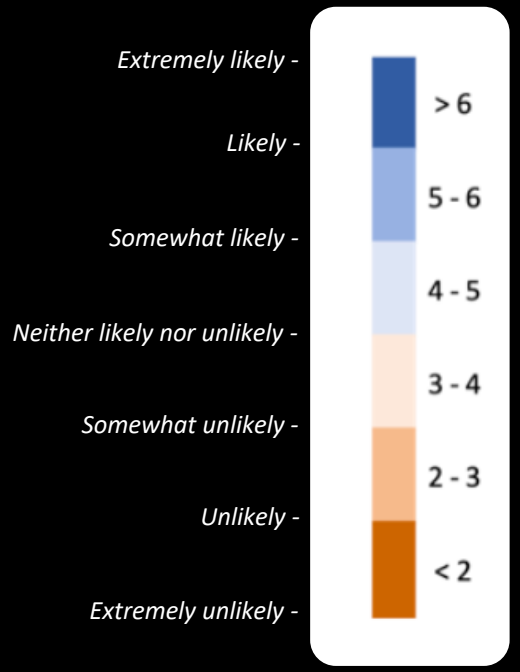
Likelihood of manufacturer responses

Security event	Connected car	IP camera	Smart Speaker	Sm. wash. machine	Smartphone	Smartwatch
No response						
DDoS	3.97	3.77	4.22	4.50	3.97	4.04
Unauthorized data access	4.10	3.94	3.88	4.44	3.76	3.82
IoT ransom attack	4.06	3.88	3.97	4.00	4.09	4.35
Inform users						
DDoS	5.12	5.00	4.96	5.41	4.79	4.58
Unauthorized data access	5.06	4.76	4.82	5.36	4.85	4.73
IoT ransom attack	4.13	4.75	5.18	4.85	4.72	4.85
Announce patch						
DDoS	5.85	5.79	5.44	5.36	5.76	5.82
Unauthorized data access	5.74	5.85	5.72	5.85	5.90	5.76
IoT ransom attack	5.68	5.44	5.53	5.36	5.73	5.91
Announce recall						
DDoS	4.61	5.03	4.82	4.50	4.73	4.56
Unauthorized data access	5.31	4.91	5.04	4.58	4.43	5.00
IoT ransom attack	5.73	4.70	4.71	4.79	4.76	4.98

RQ1: What do consumers expect how manufacturers *will* respond to emerging privacy and security risks with IoT devices?



For *security* risks, manufacturers *will* most likely patch or at least reply in some way.



"The manufacturer's response is likely."

Likelihood of manufacturer responses

Security event	Connected car	IP camera	Smart Speaker	Sm. wash. machine	Smartphone	Smartwatch
No response						
DDoS	3.97	3.77	4.22	4.50	3.97	4.04
Unauthorized data access	4.10	3.94	3.88	4.44	3.76	3.82
IoT ransom attack	4.06	3.88	3.97	4.00	4.09	4.35
Inform users						
DDoS	5.12	5.00	4.96	5.41	4.79	4.58
Unauthorized data access	5.06	4.76	4.82	5.36	4.85	4.73
IoT ransom attack	4.13	4.75	5.18	4.85	4.72	4.85
Announce patch						
DDoS	5.85	5.79	5.44	5.36	5.76	5.82
Unauthorized data access	5.74	5.85	5.72	5.85	5.90	5.76
IoT ransom attack	5.68	5.44	5.53	5.36	5.73	5.91
Announce recall						
DDoS	4.61	5.03	4.82	4.50	4.73	4.56
Unauthorized data access	5.31	4.91	5.04	4.58	4.43	5.00
IoT ransom attack	5.73	4.70	4.71	4.79	4.76	4.98

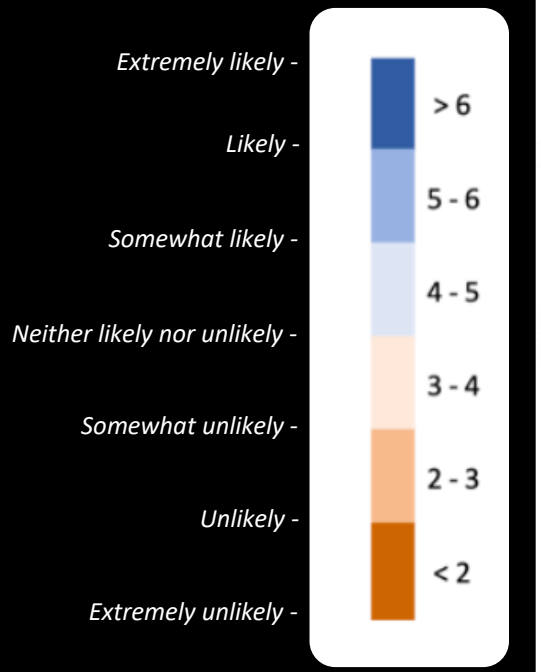
$Mean_{no\_resp.}$ = 4.05

$Mean_{inform}$ = 4.87

$Mean_{patch}$ = 5.70

$Mean_{recall}$ = 4.84

For *privacy* risks, manufacturers *will* most likely update the privacy policy (but more uncertainty than for security risks).



"The manufacturer's response is likely."

Likelihood of manufacturer responses

Privacy event	Connected car	IP camera	Smart Speaker	Sm. wash. machine	Smartphone	Smartwatch
No response						
No consent	4.14	4.28	4.60	4.66	4.28	4.52
Third party sharing	4.68	5.13	5.22	4.74	5.13	4.72
Forced data collection	4.98	4.23	4.83	4.91	5.10	4.81
Inform users via privacy policy						
No consent	5.47	5.11	5.23	5.45	5.44	5.41
Third party sharing	5.03	5.22	5.41	5.24	5.23	5.14
Forced data collection	-	-	-	-	-	-
Announce update with privacy settings						
No consent	5.18	5.15	5.21	5.14	5.24	5.29
Third party sharing	5.30	4.78	5.18	5.28	5.45	5.26
Forced data collection	5.03	5.26	5.40	5.09	5.09	5.31

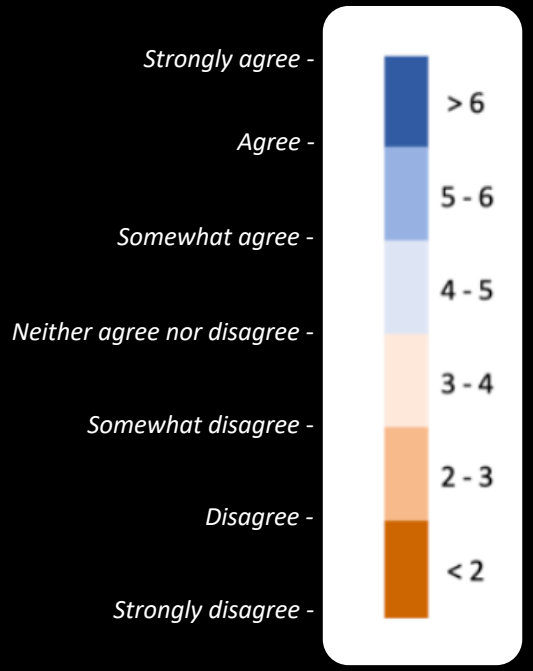
$Mean_{no\_resp.}$ = 4.74

$Mean_{inform}$ = 5.28

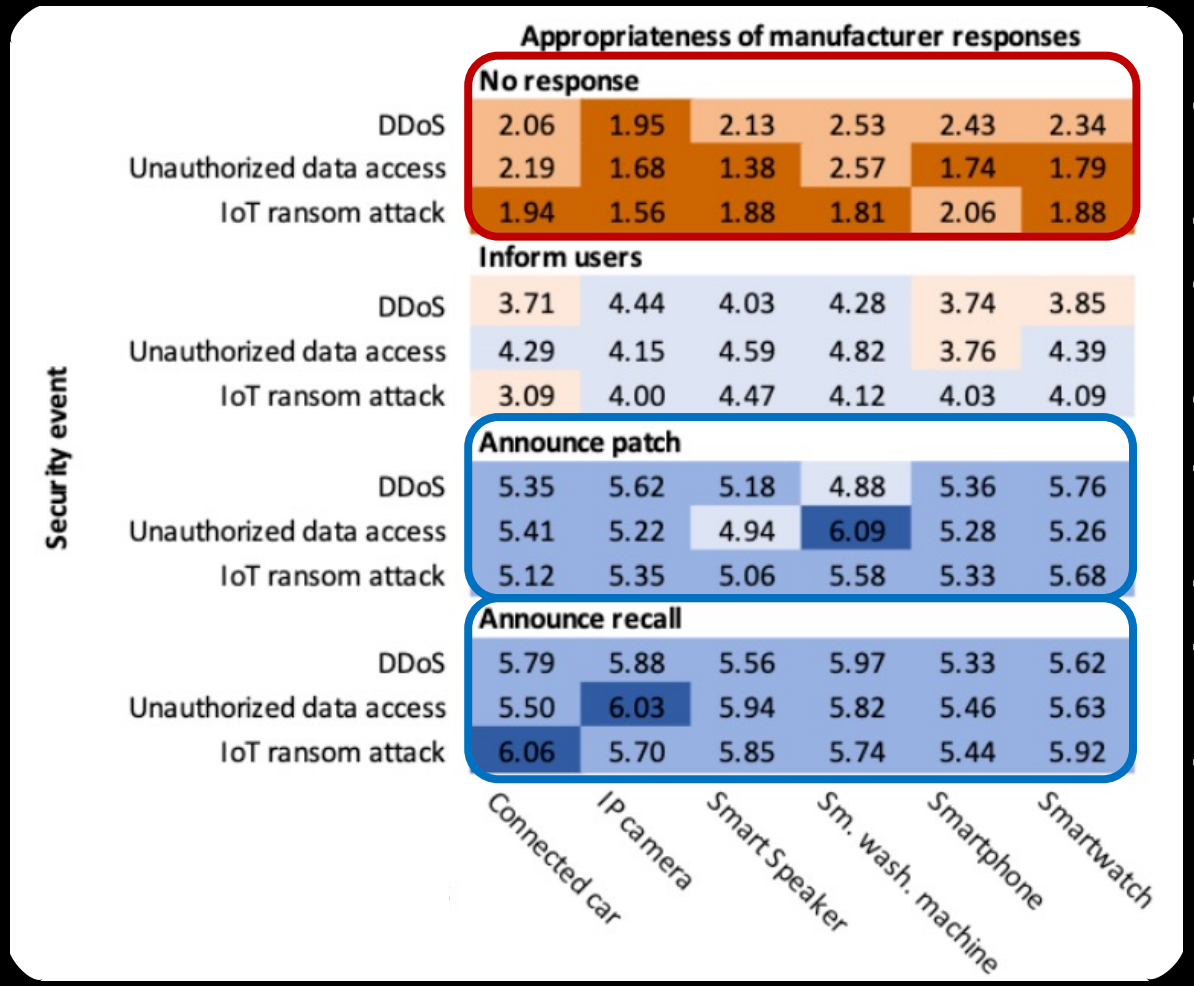
$Mean_{update}$ = 5.21

RQ2: What do consumers expect how manufacturers *should* respond to emerging privacy and security risks with IoT devices?

For *security* risks, manufacturers *should* patch and avoid response omission.



"The manufacturer's response is appropriate."



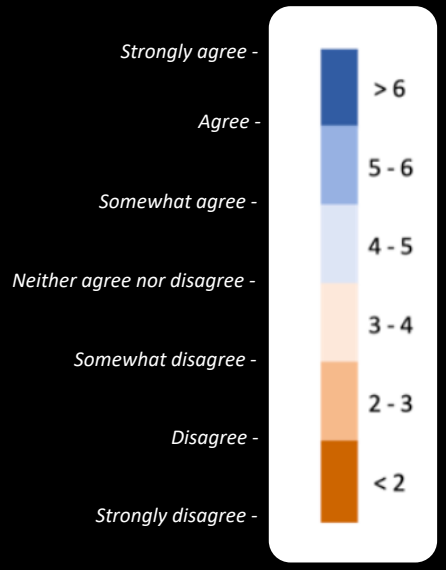
$\text{Mean}_{\text{no\_resp.}} = 2.05$

$\text{Mean}_{\text{inform}} = 4.08$

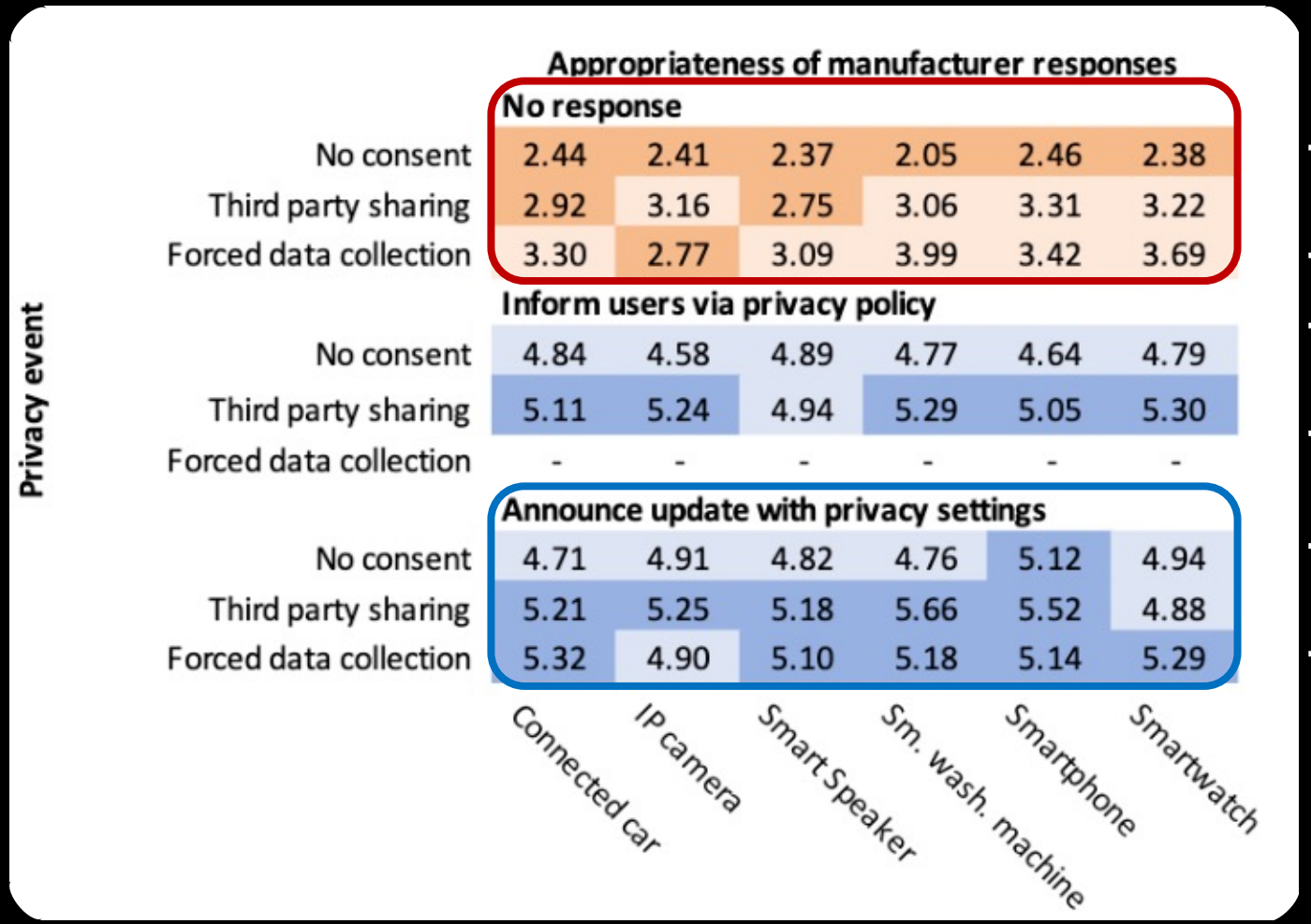
$\text{Mean}_{\text{patch}} = 5.34$

$\text{Mean}_{\text{recall}} = \underline{5.76}$

For *privacy* risks, manufacturers *should* introduce more privacy settings and avoid response omission.



"The manufacturer's response is appropriate."



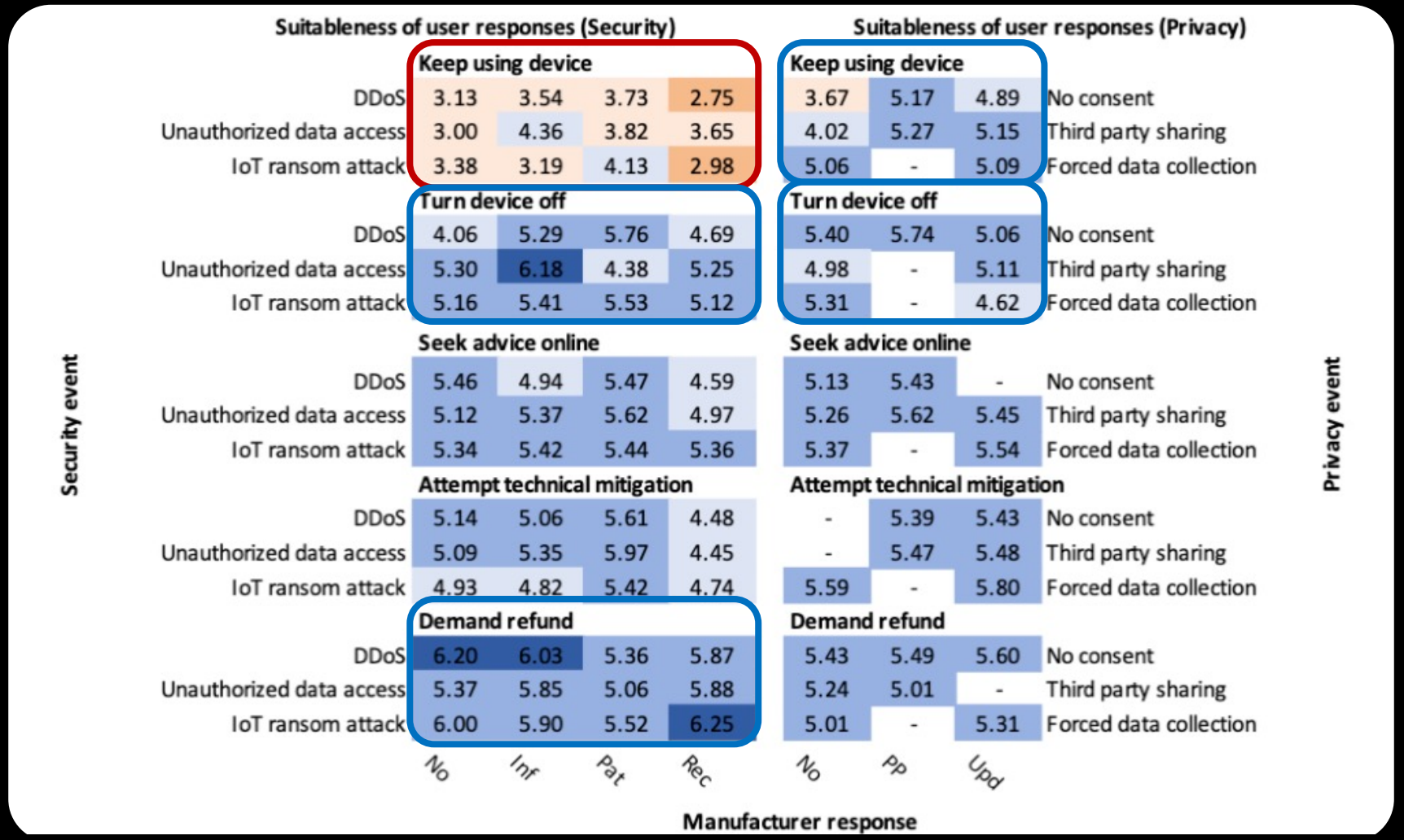
$Mean_{no\_resp.}$ = 2.95

$Mean_{inform}$ = 4.95

$Mean_{update}$ = 5.09

RQ3: How do participants evaluate the user's responsibility to handle emerging privacy and security risks with IoT devices?

For security, any user response except continued use was suitable. For privacy, continued use was seen as all right.



Implications

- Discrepancies between what consumers see as reasonable and appropriate.
- Post-purchase user support from manufacturers and governments needed.
- Empirical approach can support policymakers and legal scholars with insights into abstract legal concepts.

Summary

Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible

Lorenz Kustosch*, Carlos Gañán, Mattis van t'Schip,

Michel van Eeten, Simon Parkin

It seems reasonable to expect an IoT manufacturer to patch security flaws, but there was some resignation for privacy "flaws".

There was no clear suitable path to resolution for the user.

For questions and contact: l.f.kustosch@tudelft.nl

TU Delft Radboud University NWO