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



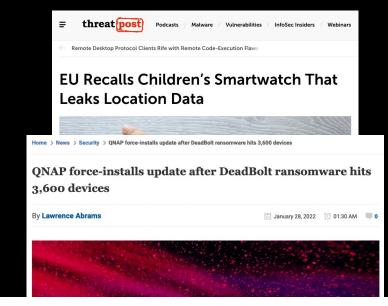
Radboud University





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.



Home > Blog

Ring Gives Videos to Police without a Warrant or User Consent

Amazon has <u>revealed</u> that it gives police videos from its Ring doorbells without a warrant and without user consent.

Consumer Expectations in IoT Security and Privacy

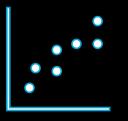
- Which rights and support can users expect when something goes wrong?
- In product liability and conformity law, the concept of "reasonable consumer expectations" can help set a baseline in regulations and court.
- But what is "reasonable" to expect about IoT security and privacy?
- Previous work focused on IoT users' preferences, e.g.,:
 - Desired security measures¹
 - Appropriate data flows²
 - Desired actor responsibilities³
- 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.

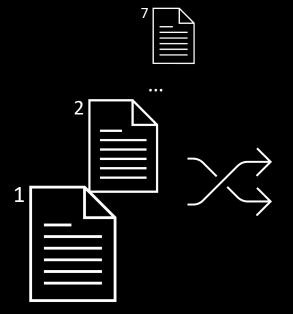
Research Questions

- (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.

Extremely unlikely	Unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Likely	Extremely likely
0	0	0	0	0	0	0

Analysis

1. Vignette factors as categorical predictors...

actors:	Alex has several [1] internet connected security cameras at home, which are kept						
1] IoT Device	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 /	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						
Privacy Event	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	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						
Response	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						

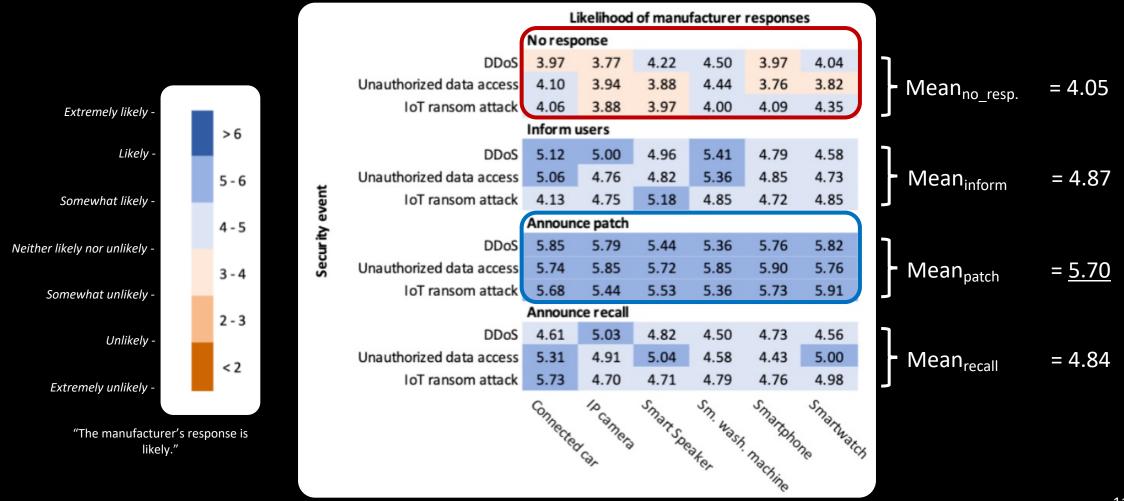
2. ... to measure effect on expectations via mean responses and regressions.

	Likelihood of manufacturer responses											
		→[Noresp									
		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				
		(
		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				
/ent		IoT ransom attack	4.13	4.75	5.18	4.85	4.72	4.85				
Security event		ſ	Announ	Announce patch								
Ľ,		DDoS	5.85	5.79	5.44	5.36	5.76	5.82				
Sec		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				
			Announ	ce recall	-							
	1	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				
		(S	10	S	Sa	Sa	S				
			Connected	IP Carnera	Part	2.42	Smartpho ma	Smartwate,				
			'ec	e's	SO.	al sh	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	no vate				
				-ar	SMar Spe	STI. Wash	Pach:					
							ne					

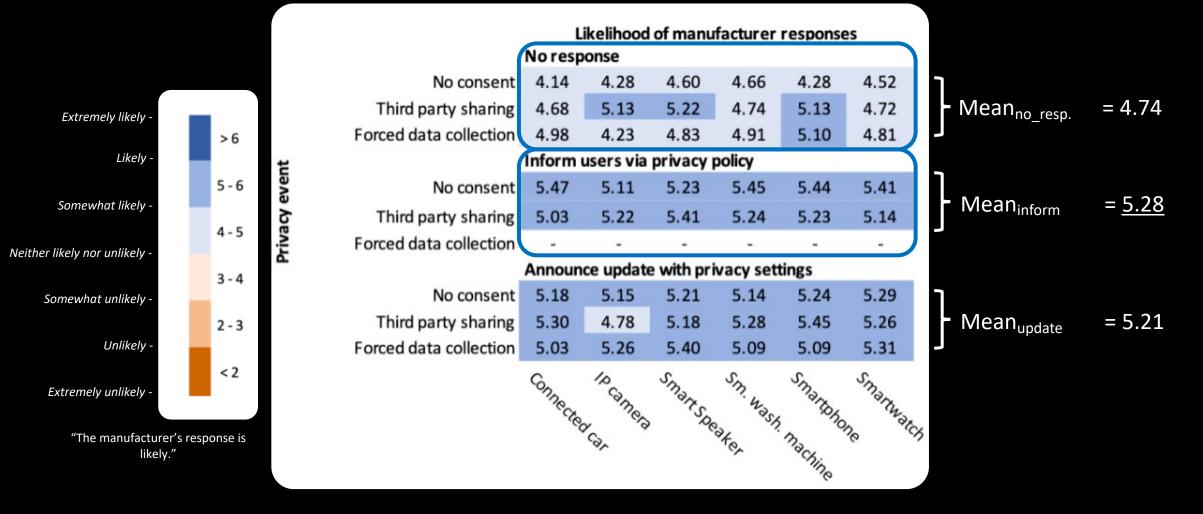
RQ1: What do consumers expect how manufacturers *will* respond to emerging privacy and security risks with IoT devices?



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



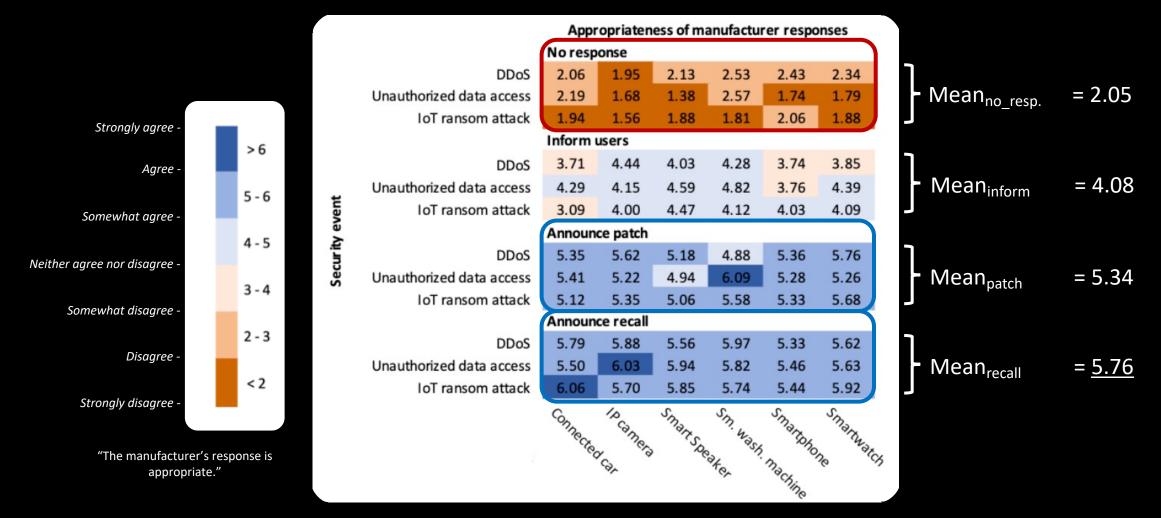
For *privacy* risks, manufacturers *will* most likely update the privacy policy (but more uncertainty than for security risks).



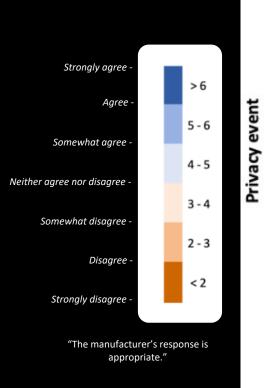
RQ2: What do consumers expect how manufacturers *should* respond to emerging privacy and security risks with IoT devices?



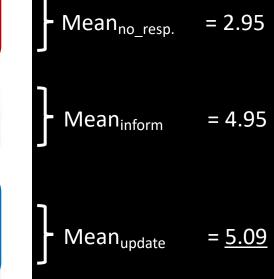
For *security* risks, manufacturers *should* patch and avoid response omission.



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



	Appropriateness of manufacturer responses											
No response												
No consent	2.44	2.41	2.37	2.05	2.46	2.38						
Third party sharing	2.92	3.16	2.75	3.06	3.31	3.22						
Forced data collection	3.30	2.77	3.09	3.99	3.42	3.69						
Inform users via privacy policy												
No consent	4.84	4.58	4.89	4.77	4.64	4.79						
Third party sharing	5.11	5.24	4.94	5.29	5.05	5.30						
Forced data collection	-					14						
Announce update with privacy settings												
No consent	4.71	4.91	4.82	4.76	5.12	4.94						
Third party sharing	5.21	5.25	5.18	5.66	5.52	4.88						
Forced data collection	5.32	4.90	5.10	5.18	5.14	5.29						
	G.	10	Smart Spe	Sa	Sa	Sa						
	nnec	IP Carnera	"ante	. 42	and	arth						
	Connected	7 ⁵ 3	De	sh.	Smattono.	Smartwater						
		A.		Str. Wash.	achip							
					0							



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.

					Suitableness of user responses (Security)						Suitableness of user responses (Privacy)				
						e			Keep using device						
					DDoS	3.13	3.54	3.73	2.75		3.67	5.17	4.89	No consent	
					Unauthorized data access	3.00	4.36	3.82	3.65		4.02	5.27	5.15	Third party sharing	
					IoT ransom attack	3.38	3.19	4.13	2.98		5.06	-	5.09	Forced data collection	
Strongly agree -					Turn device off						Turn de	vice off)	
		>6			DDoS	4.06	5.29	5.76	4.69		5.40	5.74	5.06	No consent	
Agree -					Unauthorized data access	5.30	6.18	4.38	5.25		4.98	-	5.11	Third party sharing	
		5 - 6			IoT ransom attack	5.16	5.41	5.53	5.12		5.31	-	4.62	Forced data collection	
Somewhat agree -	omewhat agree -					Seek ad	vice onlin	e			Seek advice online				
her agree nor disagree -	4 - 5		Secur ity event	DDoS	5.46	4.94	5.47	4.59		5.13	5.43		No consent	Privacy event	
ner ugree nor uisugree		3 - 4		y e	Unauthorized data access	5.12	5.37	5.62	4.97		5.26	5.62	5.45	Third party sharing	y ev
Somewhat disagree -		5-4		ur t	IoT ransom attack	5.34	5.42	5.44	5.36		5.37	-	5.54	Forced data collection	vac
	2-3				Attempt technical mitigation						Attempt	technica	l mitigati	on È	
Disagree -					DDoS	5.14	5.06	5.61	4.48		-	5.39	5.43	No consent	
		< 2			Unauthorized data access	5.09	5.35	5.97	4.45		-	5.47	5.48	Third party sharing	
Strongly disagree -					IoT ransom attack	4.93	4.82	5.42	4.74		5.59	-	5.80	Forced data collection	
					Demand refund					Demand	refund				
"Alex's response is a suitable way DDoS to move forward."		6.20	6.03	5.36	5.87		5.43	5.49	5.60	No consent					
to move for	waru.				Unauthorized data access	5.37	5.85	5.06	5.88		5.24	5.01	-	Third party sharing	
					IoT ransom attack	6.00	5.90	5.52	6.25		5.01	-	5.31	Forced data collection	
						10	Ing	Par	pec		No	20	Upg		

Neith

Manufacturer response

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





