KING'S College LONDON

Voice App Developer Experiences with Alexa and Google Assistant

Juggling Risks, Liability, and Security

William Seymour, Noura Abdi, Kopo M. Ramokapane,
Jide Edu, Guillermo Suarez-Tangil, and Jose Such

Voice Apps

Skills

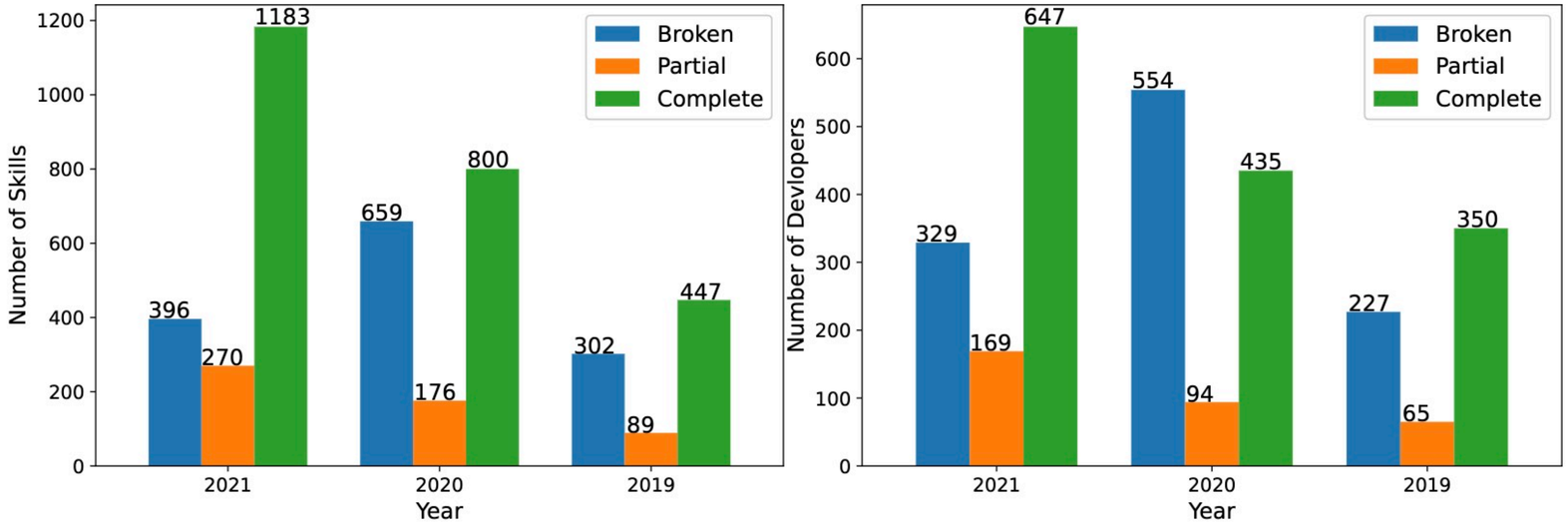
Actions

Interaction model

Certification

What's going on with assistant platforms?

Evidence of poor privacy practices



(a) Skills from 2019-2021 (b) Developers from 2019-2021

Figure 1: Traceability results for English-speaking markets.

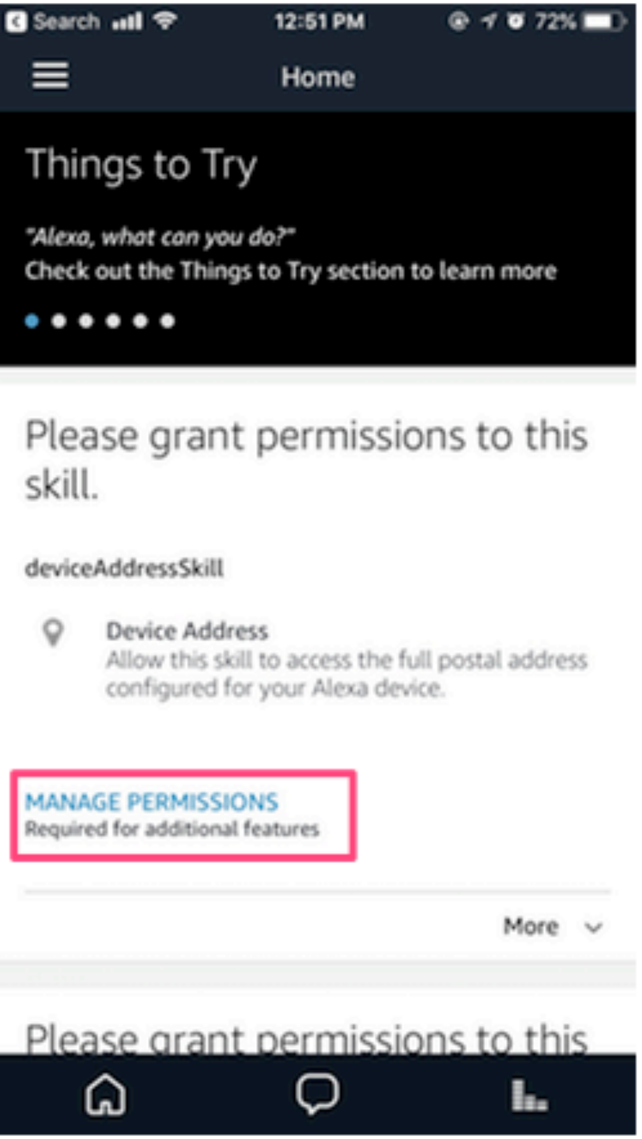
Traceability:

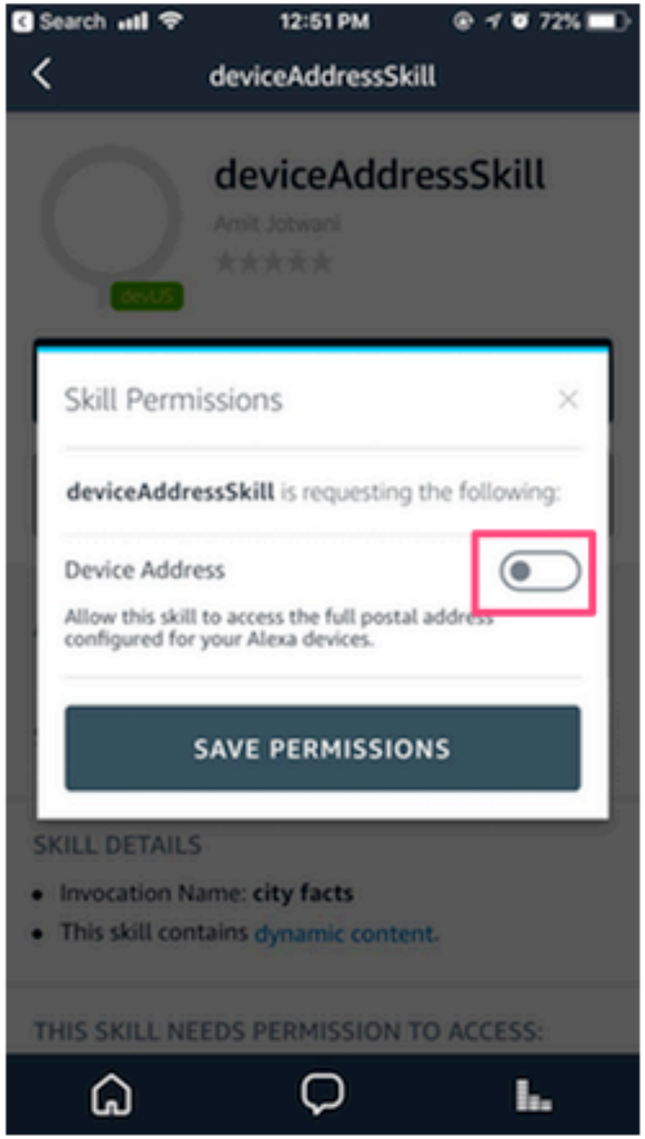
Complete

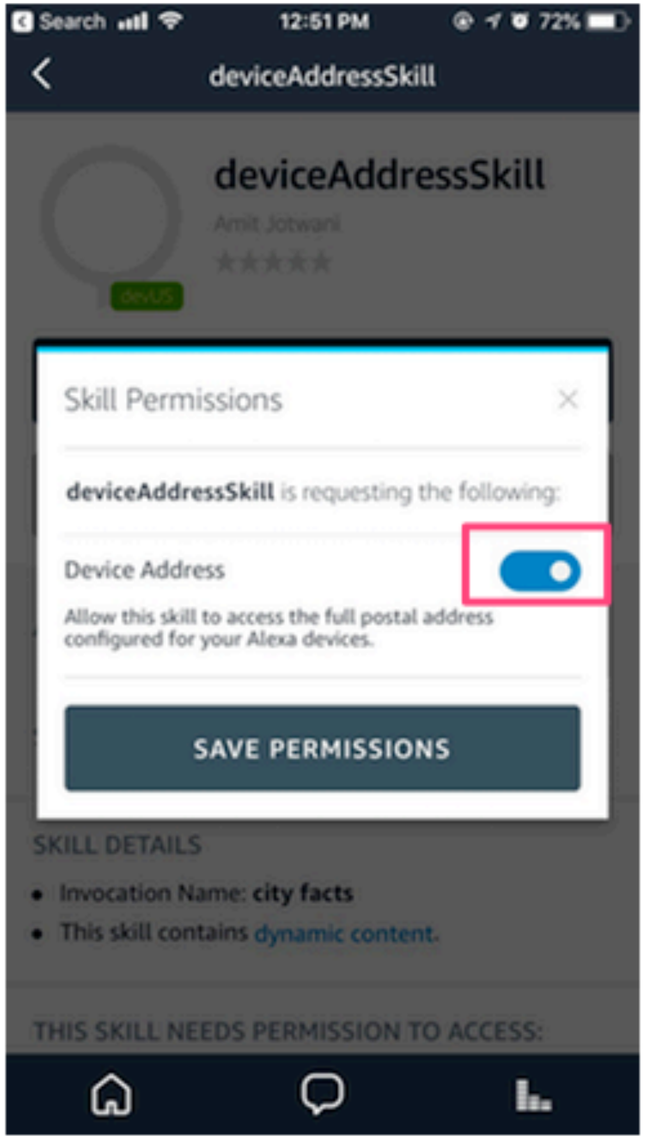
Partial

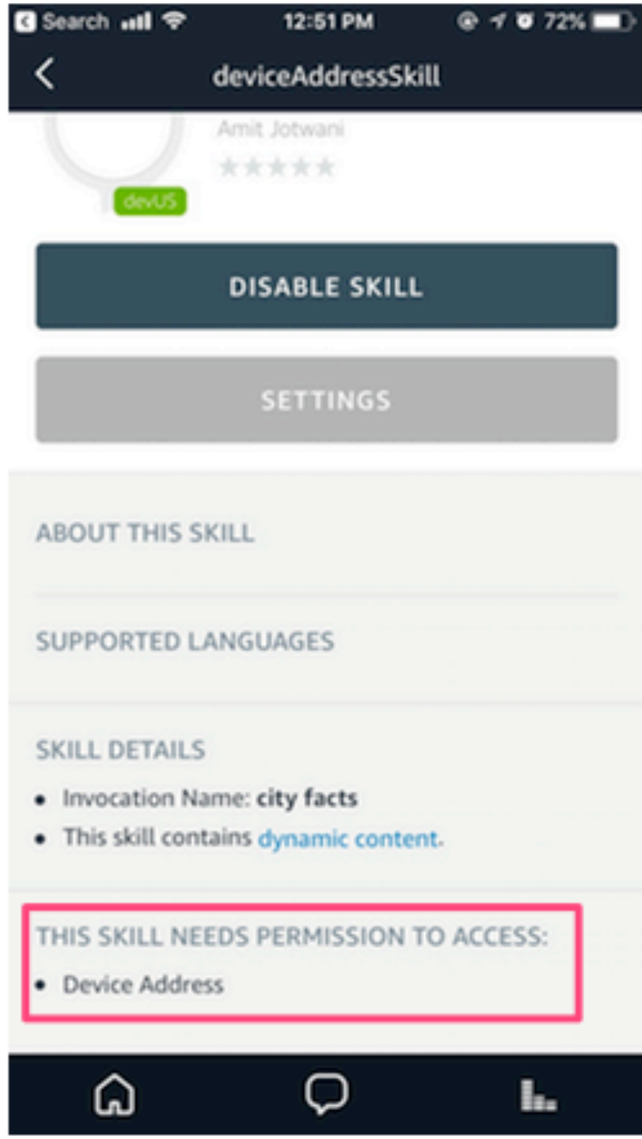
Broken

J. Edu, X. Ferrer-Aran, J. Such, and G. Suarez-Tangil. 2022. Measuring Alexa Skill Privacy Practices across Three Years. ACM Web Conference 2022 (WWW '22)


Search
12:51 PM
72%
Home
Things to Try
"Alexa, what can you do?"
Check out the Things to Try section to learn more
Please grant permissions to this skill.
deviceAddressSkill
Device Address
Allow this skill to access the full postal address configured for your Alexa device.
MANAGE PERMISSIONS
Required for additional features
More
Please grant permissions to this


Search
12:51 PM
72%
deviceAddressSkill
deviceAddressSkill
Amit Jotwani
devUS
Skill Permissions
deviceAddressSkill is requesting the following:
Device Address
Allow this skill to access the full postal address configured for your Alexa devices.
SAVE PERMISSIONS
SKILL DETAILS
Invocation Name: city facts
This skill contains dynamic content.
THIS SKILL NEEDS PERMISSION TO ACCESS:


Search
12:51 PM
72%
deviceAddressSkill
deviceAddressSkill
Amit Jotwani
devUS
Skill Permissions
deviceAddressSkill is requesting the following:
Device Address
Allow this skill to access the full postal address configured for your Alexa devices.
SAVE PERMISSIONS
SKILL DETAILS
Invocation Name: city facts
This skill contains dynamic content.
THIS SKILL NEEDS PERMISSION TO ACCESS:


Search
12:51 PM
72%
deviceAddressSkill
Amit Jotwani
devUS
DISABLE SKILL
SETTINGS
ABOUT THIS SKILL
SUPPORTED LANGUAGES
SKILL DETAILS
Invocation Name: city facts
This skill contains dynamic content.
THIS SKILL NEEDS PERMISSION TO ACCESS:
Device Address

We interact with 35k skills in the US market, excluding skills [...] We find 65 skills requesting personal information via conversation. This is 35% less than the ones found in 2020 [16].

TABLE 11
Traceability Result With `SkillVet` on Subset of Skills Found in [16] Collecting Personal Information via Conversation

How PII were collected	Traceability			Total	
	B	P	C	Skills	Dev
Conversation + Account Linking		1	6	7	5
Conversation + Alexa API		5	6	11	9
Conversation Only	35	14	33	82	79
Total number of **Skills**	35	20	45	100	–
Total number of **Developers**	35	16	40	–	89

We interact with 35k skills in market, excluding skills [...] We skills requesting personal informa conversation. This is 35% less than the ones found in 2020 [16].

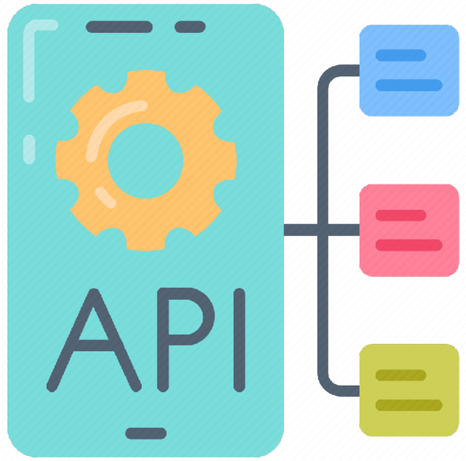
TABLE 11
ty Result With `SkillVet` on Subset of Skills Found
Collecting Personal Information via Conversation

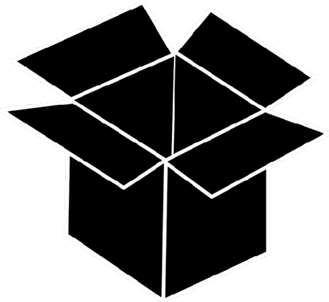
PII were collected	Traceability			Total	
	B	P	C	Skills	Dev
Conversation + Account Linking		1	6	7	5
Conversation + Alexa API		5	6	11	9
Conversation Only	35	14	33	82	79
Total number of **Skills**	35	20	45	100	–
Total number of **Developers**	35	16	40	–	89

Background - Security Certification

Interaction Model

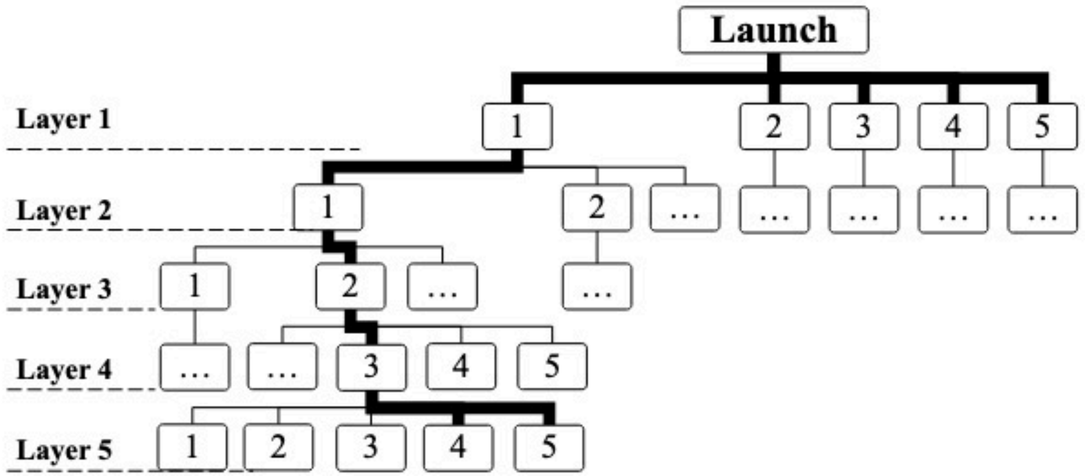
Backend



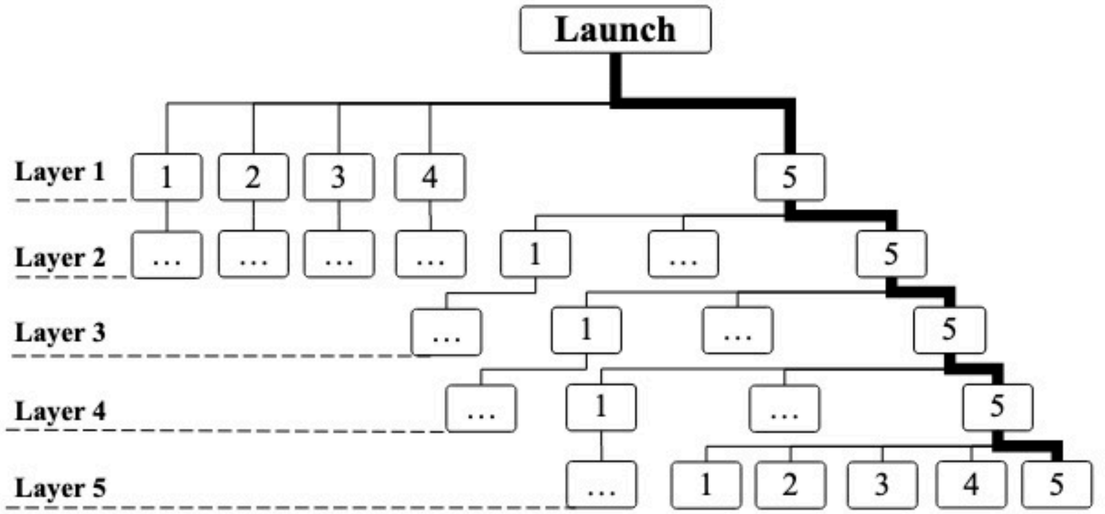


William Seymour, Mark Cote, and Jose Such. 2022. When It's Not Worth the Paper It's Written On: A Provocation on the Certification of Skills in the Alexa and Google Assistant Ecosystems. In Proceedings of the 4th Conference on Conversational User Interfaces (CUI '22). https://doi.org/10.1145/3543829.3544513

Background - Security Certification



(a) Traversal results in Amazon.



(b) Traversal results in Google.

Dawei Wang, Kai Chen, and Wei Wang. 2021. Demystifying the Vetting Process of Voice-controlled Skills on Markets. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 5, 3, Article 130 (Sept 2021), 28 pages. https://doi.org/10.1145/3478101

Background - Security Certification

interacting with VPA devices? Over a span of 15 months, we crafted and submitted for certification 234 Amazon Alexa skills and 381 Google Assistant actions that intentionally violate content and privacy policies specified by VPA platforms. Surprisingly, we successfully got 234 (100%) policy-violating Alexa skills certified and 148 (39%) policy-violating Google actions certified. Our analysis

Long Cheng, Christin Wilson, Song Liao, Jeffrey Young, Daniel Dong, and Hongxin Hu. 2020. Dangerous Skills Got Certified: Measuring the Trustworthiness of Skill Certificatio
Voice Personal Assistant Platforms. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). https://doi.org/
10.1145/3372297.3423339

What’s the Developer Experience of S&P on These Platforms?

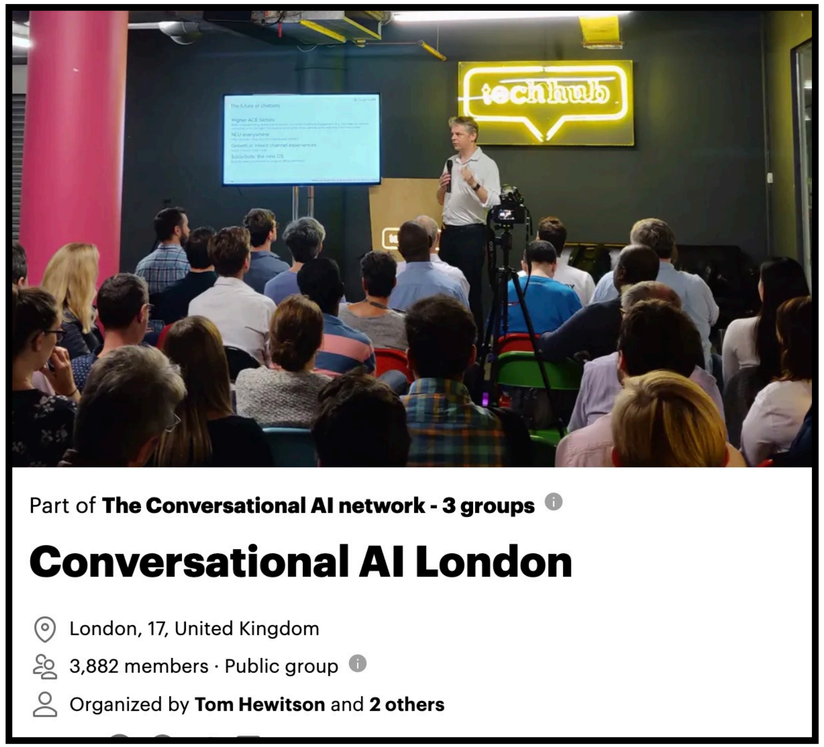
RQ1 What are the main challenges faced by voice app developers that are specific to voice app development?

RQ2 How do these challenges relate to security and privacy on voice assistant platforms?

RQ3 How do these challenges and developer responses to them differ across developers with varying levels of experience?

Reaching Developers

- 30 developers
- Publicly available contact information
- London meet-up group
- 50/50 hobbyist and professional
- Semi structured interviews
- Stopped on saturation
- 900 minutes of transcribed audio
- Analysed using thematic analysis



Money, Power & Influence

- Monetising voice apps is really difficult
- Limited advertising and poor in-app payment flows, limiting engagement
- Developer Rewards Program reduced by an order of magnitude in the past decade
- Businesses tried to diversify in order to reduce platform power
- Best option was indirect monetisation

Risk & Liability

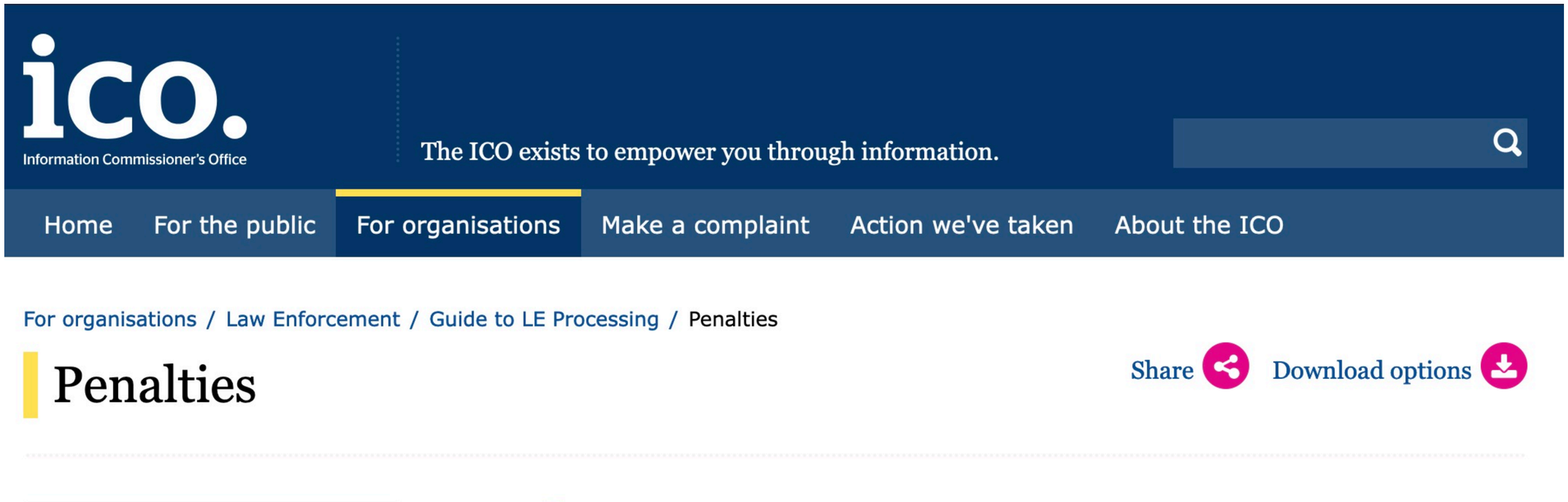
“they also even give us advance notice of certain things that they’re going to develop” [P20]

“we get really buggy beta functionality for Amazon. That then goes into certification process and the certification team haven’t been briefed on the functionality” [P23]

Privacy

“I found some really good privacy policies online and copied them” [P06]

“my approach there was always just to send a link to [the client’s] privacy policy, just the one that’s linked on their website” [P22]



Security

Submission checklist

To prepare your skill for the certification process, review the following certification requirements.

1. Policy Requirements for Alexa Skills – The policy guidelines make sure that your skill is appropriate for all customers. Adherence to these guidelines guards the privacy and welfare of Alexa users.

2. Security Requirements for Alexa Skills – Customer trust is important to Amazon. To protect customer data, your skill must meet these security requirements.

3. Requirements for Skills that Allow Purchases – All Alexa skills that allow users to make a purchase must adhere to these requirements.

4. Requirements for Skills that are HIPAA-Eligible – All Alexa skills that process Protected Health Information (PHI) must comply with these requirements.

5. Alexa Advertising ID Policy – All Alexa skills that use Alexa advertising ID for analytics and advertising must meet these policy requirements.

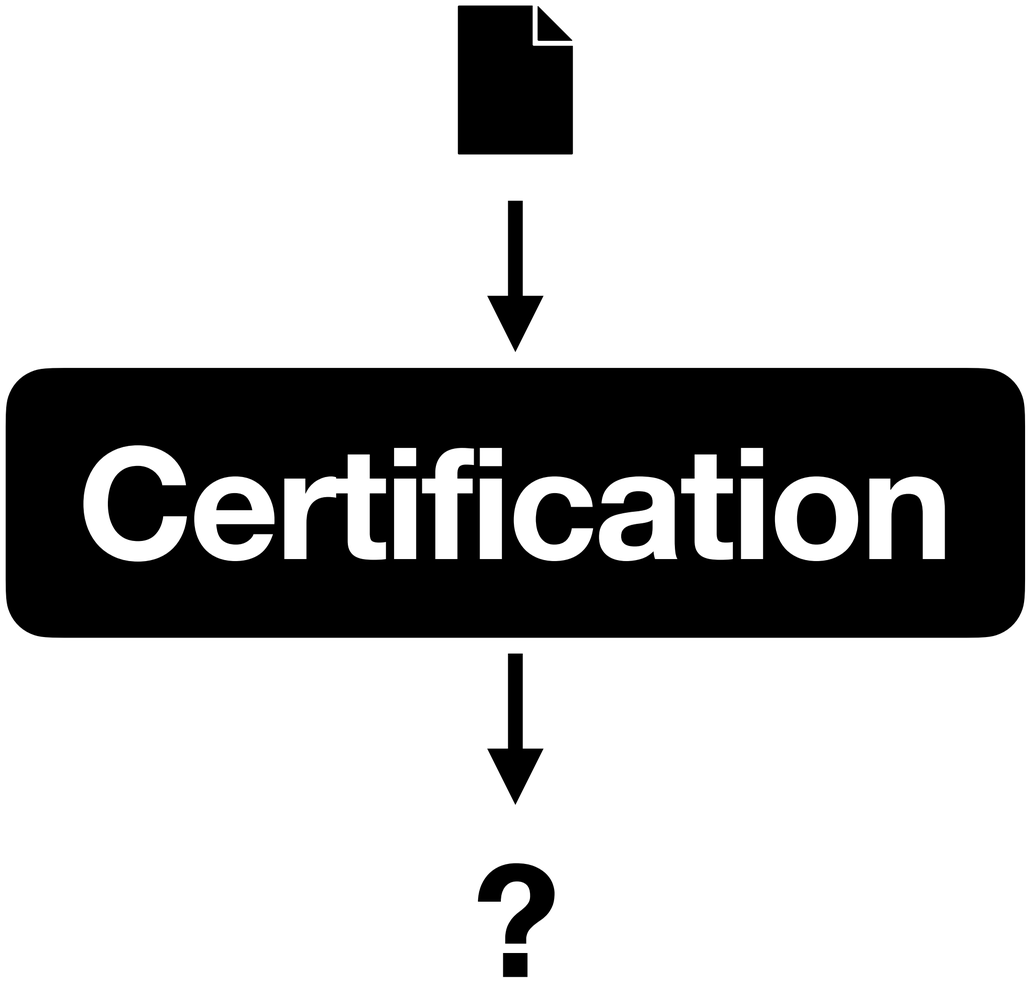
6. Perform all required skill certification tests.

Certification

Certification

- Inconsistent turnaround
- Inconsistent results between past and future certifications
- Inconsistent results between certification in different markets
- This led to widespread attempts to avoid (re)certification

“*we do have people within Amazon that can be very useful and kind to us [..] if you’ve got a couple of people’s email addresses in Amazon, you can sometimes wiggle it. We try not to do it too often.*” [P23]



Takeaways

1. Voice makes it *really hard* to reuse existing designs and processes

2. Platforms need to be architected around certification

3. Platforms “optimise out” responsibility for privacy & security

4. Hard to do quantitative research given inconsistent processes

william.1.seymour@kcl.ac.uk