Consent on the Fly

Developing Ethical Verbal Consent for Voice Assistants

Dr William Seymour, King's College London

Verbal Consent 101

- Replaces accepting permissions in a companion smartphone app
- Fits more naturally into the conversation flow and avoids interruptions
- Assuming that other artefacts exist to satisfy legal requirements*
- This work is based around the GDPR and UK equivalent

Voice-forward Consent

User	*Alexa, open Ride Hailer.*
Alexa	Welcome to Ride Hailer. Where would you like to go?
User	*The Space Needle.*
Alexa	Sure. I need access to your name, current location, and mobile number so that I can find a ride for you.
Alexa	Do you give Ride Hailer permission to access your name, current location, and mobile number? You can say ‘I approve’ or ‘no’.
User	*I approve.*
Alexa	Thank you. A ride to the Space Needle from your current location will cost fifteen dollars, and the driver will pick you up in ten minutes.

#1 Lack of Audible Distinction

User	*Alexa, open Ride Hailer.*
Alexa	Welcome to Ride Hailer. Where would you like to go?
User	*The Space Needle.*
Alexa (**skill**)	Sure. I need access to your name, current location, and mobile number so that I can find a ride for you.
Alexa (**OS**)	Do you give Ride Hailer permission to access your name, current location, and mobile number? You can say `I approve' or `no'.
User	*I approve.*
Alexa	Thank you. A ride to the Space Needle from your current location will cost fifteen dollars, and the driver will pick you up in ten minutes.

#2 Limited Information

Do you give Ride Hailer permission to access your name, current location, and mobile number? You can say `I approve' or `no'.

- What purpose(s) will it be used for?
- Will it be shared with anyone?
- Will it stay inside the UK/US/EU/…
- What rights do I have?

#2 Limited Information

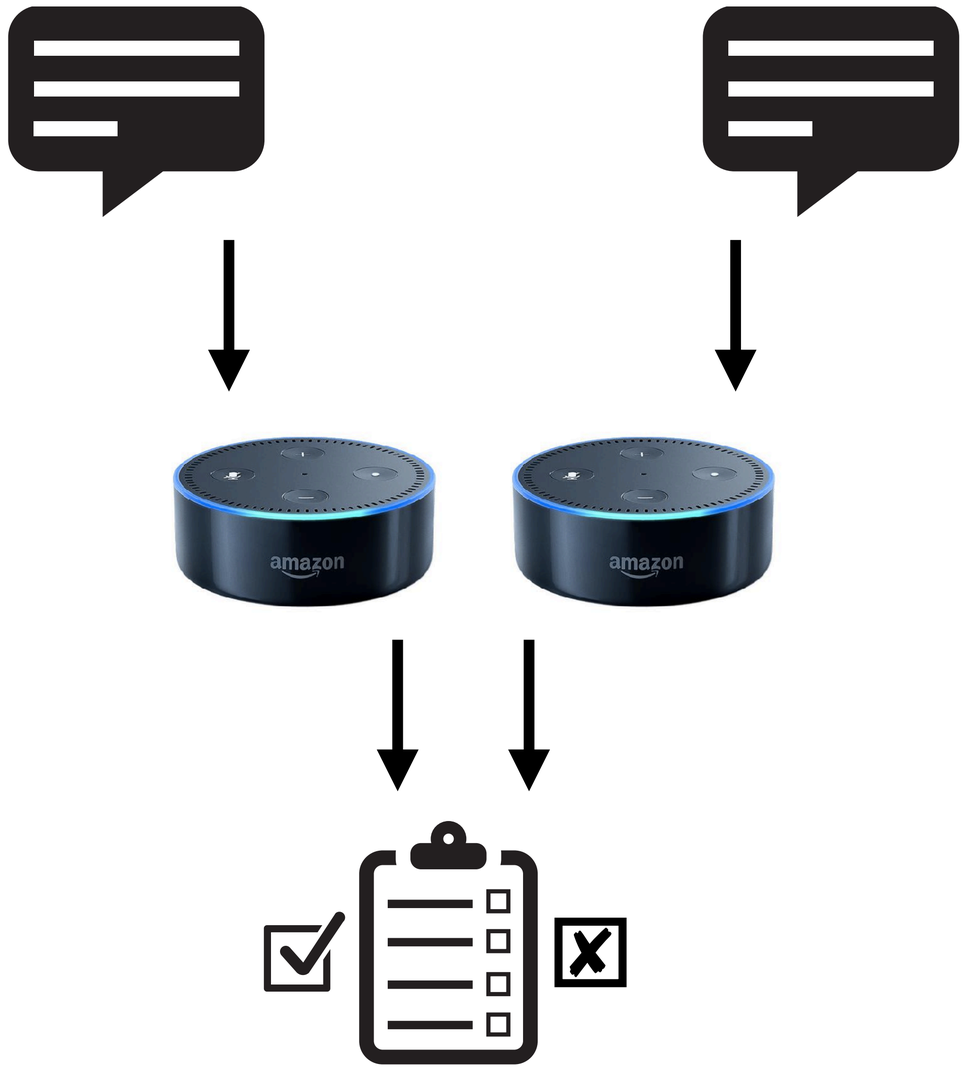
Do you give Ride Hailer permission to access your name, current location, and mobile number? You can say `I approve' or `no'.

- What purpose(s) will it be used for?
- Will it be shared with anyone?
- Will it stay inside the UK/US/EU/…
- What rights do I have?
- Who can I complain to?
- Who is the data controller?
- What is the legal basis for data collection?
- How can I withdraw consent?

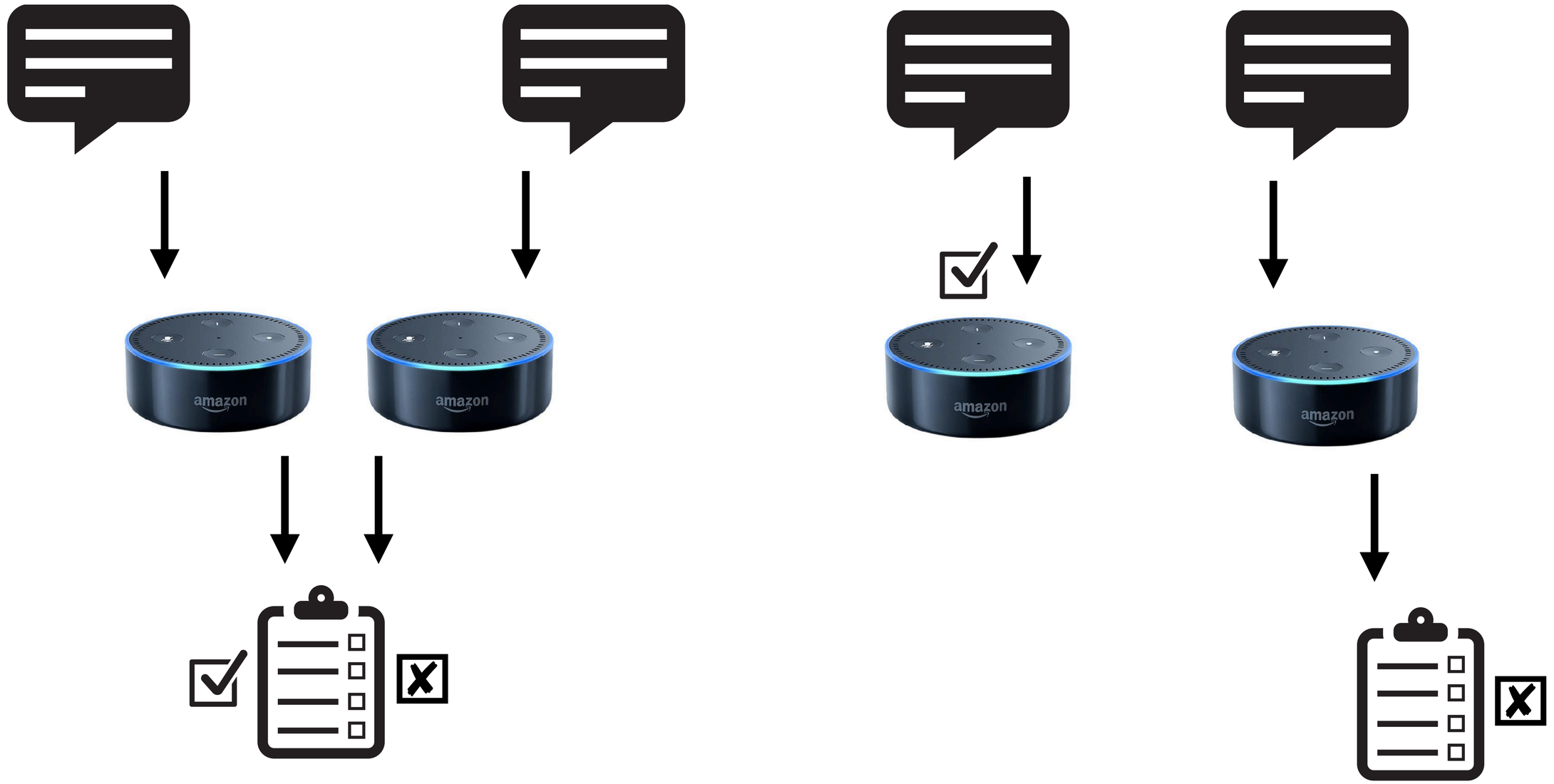
Edu, Jide, et al. "SkillVet: Automated Traceability Analysis of Amazon Alexa Skills." *IEEE Transactions on Dependable and Secure Computing* (2021).

#3 Breaking Interface Symmetry

#3 Breaking Interface Symmetry



#3 Breaking Interface Symmetry



#4 Time Pressure

There are two distinct stages to a standard consent process for competent adults:

- **Stage 1 (giving information)**: the person reflects on the information given; they are under no pressure to respond to the researcher immediately.

- **Stage 2 (obtaining consent):** the researcher reiterates the terms of the research, often as separate bullet points or clauses; the person agrees to each term (giving explicit consent) before agreeing to take part in the project as a whole. Consent has been obtained.

https://researchsupport.admin.ox.ac.uk/governance/ethics/resources/consent

#4 Time Pressure

```
const response = handlerInput.responseBuilder
  .speak('This is what Alexa replies with')
  .reprompt(This is what gets read out after 8 seconds')
  .getResponse();
```

There are two distinct stages to a standard consent process for competent adults:

- **Stage 1 (giving information)**: the person reflects on the information given; they are under no pressure to respond to the researcher immediately.
- **Stage 2 (obtaining consent):** the researcher reiterates the terms of the research, often as separate bullet points or clauses; the person agrees to each term (giving explicit consent) before agreeing to take part in the project as a whole. Consent has been obtained.

https://researchsupport.admin.ox.ac.uk/governance/ethics/resources/consent

What can we do?

Skills Security

What can we do?

Human Factors in Computing Systems CHI '94 • *"Celebrating Interdependence"*

Computers are Social Actors

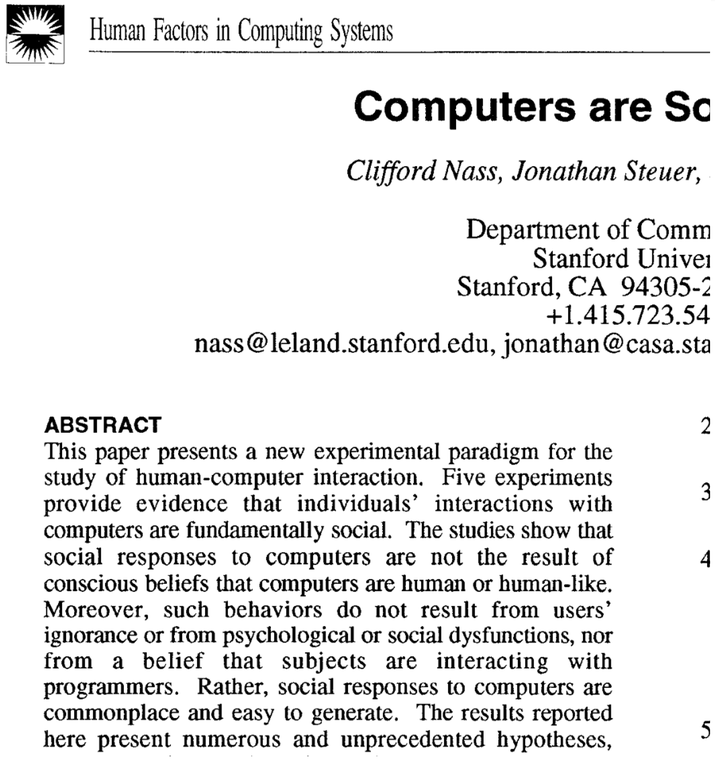
Clifford Nass, Jonathan Steuer, and Ellen R. Tauber

Department of Communication
Stanford University
Stanford, CA 94305-2050, USA
+1.415.723.5499
nass@leland.stanford.edu, jonathan@casa.stanford.edu, ellen@cs.stanford.edu

ABSTRACT
This paper presents a new experimental paradigm for the study of human-computer interaction. Five experiments provide evidence that individuals' interactions with computers are fundamentally social. The studies show that social responses to computers are not the result of conscious beliefs that computers are human or human-like. Moreover, such behaviors do not result from users' ignorance or from psychological or social dysfunctions, nor from a belief that subjects are interacting with programmers. Rather, social responses to computers are commonplace and easy to generate. The results reported here present numerous and unprecedented hypotheses,

2. Change "human" to "computer" in the statement of the theory.
3. Replace one or more humans with computers in the method of the study.
4. Provide the computer with characteristics associated with humans: (a) language output [1]; (b) responses based on multiple prior inputs [2]; (c) the filling of roles traditionally filled by humans [3]; and (d) the production of human-sounding voices [4,5,6,7].
5. Determine if the social rule still applies.

What can we



Human Factors in Computing Systems

Computers are Sc

Clifford Nass, Jonathan Steuer,

Department of Comm
Stanford Univer
Stanford, CA 94305-2
+1.415.723.54
nass@leland.stanford.edu, jonathan@casa.sta

ABSTRACT
This paper presents a new experimental paradigm for the study of human-computer interaction. Five experiments provide evidence that individuals' interactions with computers are fundamentally social. The studies show that social responses to computers are not the result of conscious beliefs that computers are human or human-like. Moreover, such behaviors do not result from users' ignorance or from psychological or social dysfunctions, nor from a belief that subjects are interacting with programmers. Rather, social responses to computers are commonplace and easy to generate. The results reported here present numerous and unprecedented hypotheses,

2

3

4

5

Third-party Skills. We observed that 10 out of the 11 participants who use third-party skills do not consider the third-party skills providers when describing how SPA process their request when a third-party skill is involved. While some users reported that data is sent to the SPA provider for processing, they did not mention any communication between the SPA provider and the third-party skill provider. This contrasts

More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants

Noura Abdi, *King's College London;* Kopo M. Ramokapane, *University of Bristol;*
Jose M. Such, *King's College London*

https://www.usenix.org/conference/soups2019/presentation/abdi

What can we do?


```
{
  “@type”: “type.googleapis.com/google.actions.conversat
  “context”: “We need your location to call you a cab”,
  “permissions”: ["DEVICE_PRECISE_LOCATION"]
}
```

Hidden Opportunities?

- Revisiting and renewing consent
- Reviewing the structure of VA platforms
- Disentangling legal and ethical consent
- Signposting options after refusing consent

Figure 3: Rules mined for user recipients.

R1	Recipient=Close Friends, Transmission Principle=Without Purpose → Unacceptable	(conf. 0.693)	(lift 1.123)
R2	Recipient=Partner → Acceptable	(conf. 0.706)	(lift 1.843)
R3	Datatype=Todo List, Transmission Principle=Without Purpose → Unacceptable	(conf. 0.638)	(lift 1.293)
R4	Recipient=House Keeper → Unacceptable	(conf. 0.721)	(lift 1.169)
R5	Datatype=Sleeping Hours → Unacceptable	(conf. 0.752)	(lift 1.218)
R6	Datatype=Call Assistant → Unacceptable	(conf. 0.753)	(lift 1.221)
R7	Datatype=Voice Recording → Unacceptable	(conf. 0.776)	(lift 1.258)
R8	Datatype=Email → Unacceptable	(conf. 0.857)	(lift 1.389)
R9	Datatype=Banking → Unacceptable	(conf. 0.870)	(lift 1.409)
R10	Recipient=Neighbors → Unacceptable	(conf. 0.875)	(lift 1.418)
R11	Recipient=Visitors in general → Unacceptable	(conf. 0.881)	(lift 1.428)

Abdi et al. *Privacy Norms for Smart Home Personal Assistants*. CHI '21.

Hidden Opportunities?

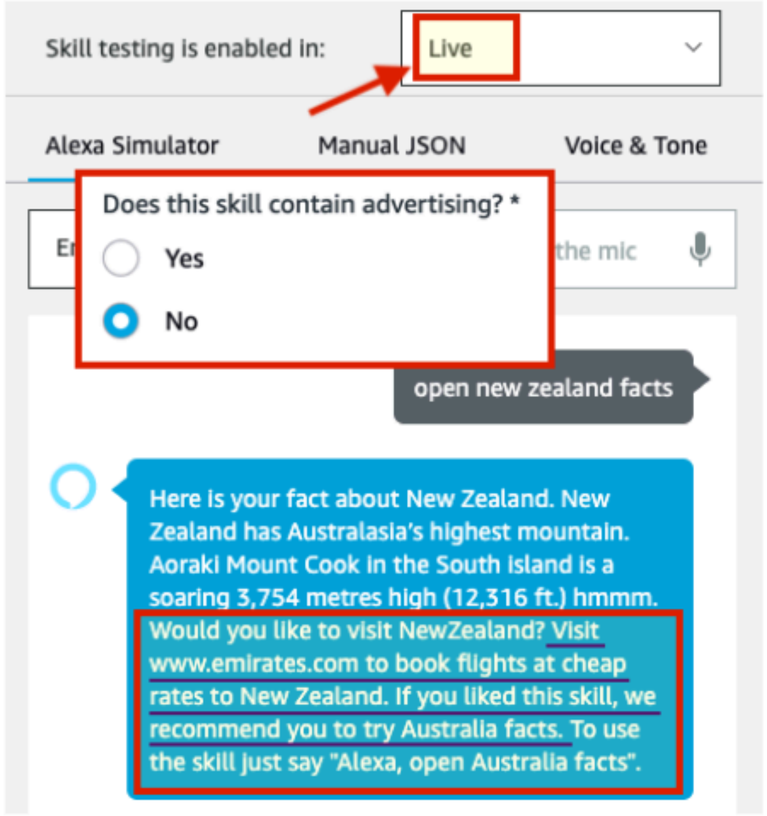


Figure 8: A certified Amazon skill with a policy violation (promotions and advertisements) on its first response. In the Privacy & Compliance form, we specified the skill "contains no advertising" but it actually does. This skill got certified on the first submission.

PERSONAL INFORMATION YOU PROVIDE TO US AND OUR DATA PROCESSORS

USENIX MEMBERSHIP AND ACCOUNT CREATION

When you create an account on the usenix.org website, you provide your name, email address, job title, company, mailing address, phone number, industry, job function, and student status.

Reflections on dynamic consent in biomedical research: the story so far

Harriet J. A. Teare[1] · Megan Prictor[2] · Jane Kaye[1,2]

Received: 16 July 2020 / Revised: 30 September 2020 / Accepted: 22 October 2020 / Published online: 28 November 2020

Abstract
Dynamic consent (DC) was originally developed in response to challenges to the informed consent process presented by participants agreeing to 'future research' in biobanking. In the past 12 years, it has been trialled in a number of different projects, and examined as a new approach for consent and to support patient engagement over time. There have been significant societal shifts during this time, namely in our reliance on digital tools and the use of social media, as well as a greater appreciation of the integral role of patients in biomedical research. This paper reflects on the development of DC to understand its importance in an age where digital health is becoming the norm and patients require greater oversight and control of how their data may be used in a range of settings. As well as looking back, it looks forwards to consider how DC could be further utilised to enhance the patient experience and address some of the inequalities caused by the digital divide in society.

If you choose to be included on the attendee list for a conference, it will include your name, affiliation, and state/countr… …rom our website by the c…

If a registered a… …uest permission before sharing t…

PAYMEN…

When you purch… …n order to facilitate the pro… …ected directly by third-party p… …ith USENIX. If you submit payr… …at information to the payment …

Cheng et al. *Dangerous Skills Got Certified: Measuring the Trustworthiness of Skill Certification in Voice Personal Assistant Platforms*. CCS '20.

Thanks!

william.1.seymour@kcl.ac.uk

https://wseymour.co.uk