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
Welcome to Ride Hailer. Where would you like to go?

The Space Needle.

Sure. I need access to your name, current location, and mobile number so that I can find a ride for you.

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

I approve.

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. |
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

EVALUATION

ADVICE

OPTIONS

EVALUATION
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
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

Stop
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

Computers are Social
Clifford Nass, Jonathan Steuer,
Department of Comm.
Stanford Unive;
Stanford, CA 94305-2
+1.415.723.54
nass@leland.stanford.edu, jonathan@cas.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,

Third-party Skills. We observed that 10 out of the 11 par-
ticipants 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 process-
ing, 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.conversation.v3.PermissionValueSpec", "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

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.

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