Evaluating the Contextual Integrity of Privacy Regulations: Parents' IoT Toy Privacy Norms Versus COPPA

Noah Apthorpe, Sarah Varghese, Nick Feamster

COPPA & “Smart” Toys

- FTC updated its Children’s Online Privacy Protection Act (COPPA) guidance in 2017 to include “connected toys or other Internet of Things devices”




Gray, S. Federal Trade Commission: COPPA Applies to Connected Toys. *Future of Privacy Forum* (June 2017)

Research Questions

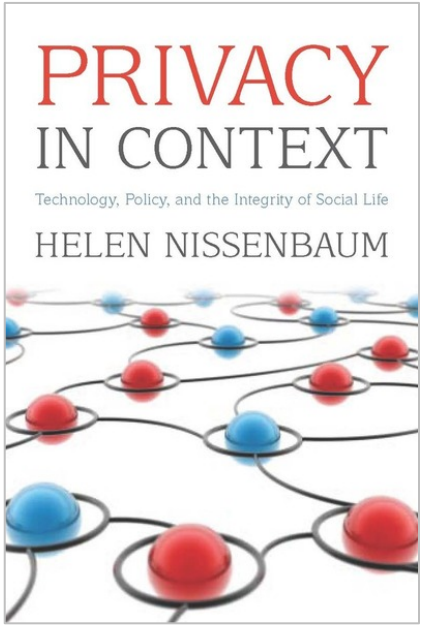
- Do COPPA-mandated data handling practices for smart toys align with parents' privacy norms?

And more generally…

- How can we test whether privacy regulations align with social and cultural privacy norms?

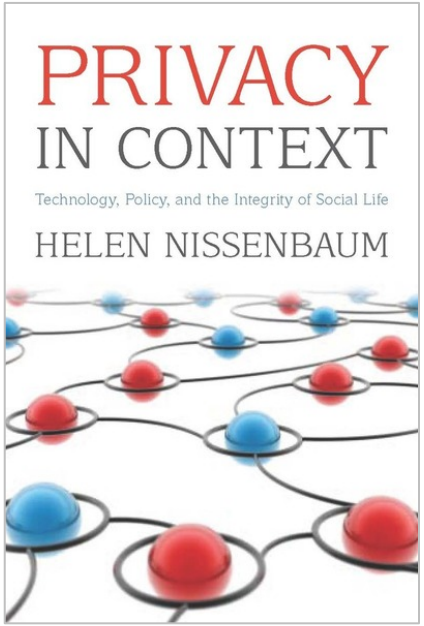
Defining Privacy Norms

- Contextual integrity (CI)
  - Privacy as norms of information flow appropriateness in specific contexts



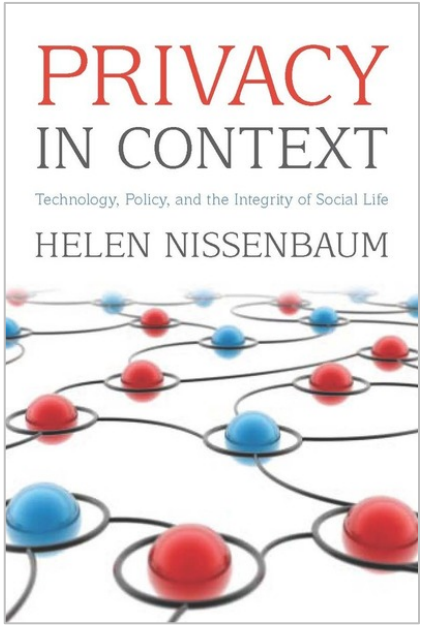
Defining Privacy Norms

- Contextual integrity (CI)
  - Privacy as norms of information flow appropriateness in specific contexts
  - Contexts and associated norms are described by **5 parameters**
    - Sender, subject, attribute (information type), recipient, transmission principle



Defining Privacy Norms

- Contextual integrity (CI)
  - Privacy as norms of information flow appropriateness in specific contexts
  - Contexts and associated norms are described by **5 parameters**
    - Sender, subject, attribute (information type), recipient, transmission principle
    - A doctor may share a patient's medical records with another hospital for continuity of care



Measuring Privacy Norms: CI Survey Method

Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity

NOAH APTHORPE, Princeton University, USA
YAN SHVARTZSHNAIDER, New York University, USA and Princeton University, USA
ARUNESH MATHUR, Princeton University, USA
DILLON REISMAN, Princeton University, USA
NICK FEAMSTER, Princeton University, USA

The proliferation of Internet of Things (IoT) devices for consumer "smart" homes raises concerns about user privacy. We present a survey method based on the Contextual Integrity (CI) privacy framework that can quickly and efficiently discover privacy norms at scale. We apply the method to discover privacy norms in the smart home context, surveying 1,731 American adults on Amazon Mechanical Turk. For $2,800 and in less than six hours, we measured the acceptability of 3,840 information flows representing a combinatorial space of smart home devices sending consumer information to first and third-party recipients under various conditions. Our results provide actionable recommendations for IoT device manufacturers, including design best practices and instructions for adopting our method for further research.

Apthorpe, et al. "Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity." *IMWUT/Ubicomp*. 2018

Measuring Privacy Norms vs Regulation: Modified CI Survey Method

1. Choose parameter values from regulation (COPPA)
2. Generate questions about acceptability of 1056 5-parameter information flows
3. Test survey with cognitive interviews
4. Deploy survey to 195 U.S. parents of children ages 3-13
5. Group responses by parameter & demographics
6. Compare acceptability scores across groups

Measuring Privacy Norms vs Regulation: Modified CI Survey Method

1. Choose parameter values from regulation (COPPA)

Sender
- a toy walkie-talkie
- a smart doll
- a toy robot
- …

Subject & Attribute
- its owner's child's location
- audio of its owner's child
- its owner's child's birthday
- …

Recipient
- its manufacturer
- a third-party service provider

Measuring Privacy Norms vs Regulation: Modified CI Survey Method

1. Choose parameter values from regulation (COPPA)

Transmission principles from FTC's 6-step COPPA compliance plan

- if its privacy policy permits it
- if its owner has given verifiable consent
- if it implements reasonable procedures to protect the information collected
- if the information is stored for as long as is reasonably necessary for the purpose for which it was collected
- …

Include *null* (no-criteria) transmission principle as control

Measuring Privacy Norms vs Regulation: Modified CI Survey Method

2. Generate combinations of 5 parameters to create 1056 questions about information flow acceptability

Null transmission principle (no COPPA conditions)

A **toy walkie-talkie** records **the times it is used**. How acceptable is it for the toy walkie-talkie to send this information to the following recipients?

	Completely unacceptable	Somewhat unacceptable	Neutral	Somewhat acceptable	Completely acceptable	Doesn't make sense
its manufacturer	○	○	○	○	○	○
a third-party service provider	○	○	○	○	○	○

Measuring Privacy Norms vs Regulation: Modified CI Survey Method

2. Generate combinations of 5 parameters to create 1056 questions about information flow acceptability

A **toy walkie-talkie** records **the times it is used**. How acceptable is it for the toy walkie-talkie to send this information to **its manufacturer** under the following conditions?

COPPA transmission principles

	Completely unacceptable	Somewhat unacceptable	Neutral	Somewhat acceptable	Completely acceptable	Doesn't make sense
if the information is stored for as long as is reasonably necessary for the purpose for which it was collected	○	○	○	○	○	○
if the information is deleted	○	○	○	○	○	○

Measuring Privacy Norms vs Regulation: Survey Testing & Deployment

3. Testing
   - Cognitive interviews (screen recordings & audio feedback) with pilot respondents

*https://www.cint.com

Measuring Privacy Norms vs Regulation: Survey Testing & Deployment

3. Testing
   - Cognitive interviews (screen recordings & audio feedback) with pilot respondents

4. Deployment
   - 195 U.S. parents of children ages 3-13
   - Recruited respondents via Cint*

*https://www.cint.com

Measuring Privacy Norms vs Regulation: Response Analysis

5. Group responses by
   - Individual parameters
     - E.g. all questions with recipient “its manufacturer”
   - Pairs of parameters
     - E.g. all questions with “its manufacturer” **and** “if it’s privacy policy permits it”
   - Participant demographics

Measuring Privacy Norms vs Regulation: Response Analysis

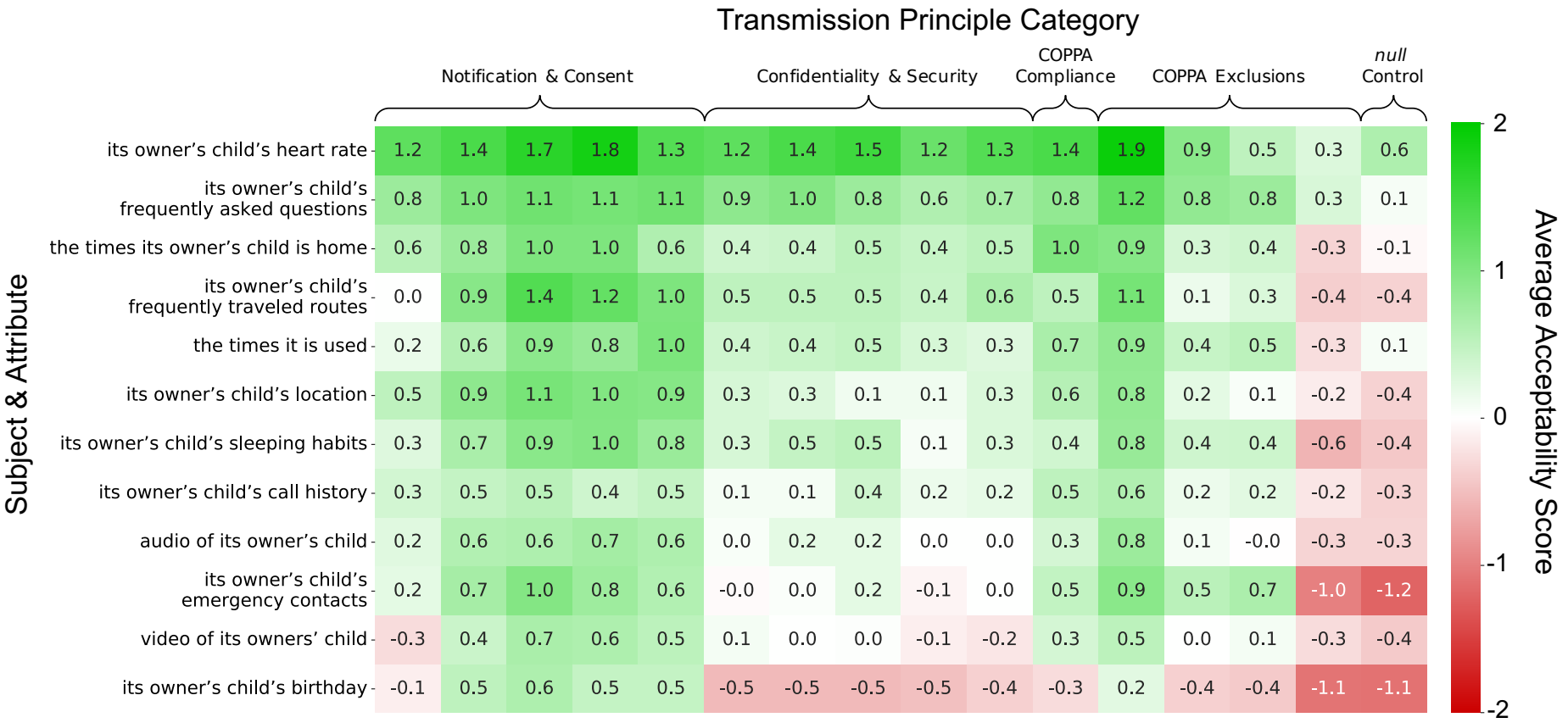
5. Group responses by
   - Individual parameters
     - E.g. all questions with recipient “its manufacturer”
   - Pairs of parameters
     - E.g. all questions with “its manufacturer” **and** “if it’s privacy policy permits it”
   - Participant demographics

6. Compare Likert acceptability scores across groups
   - Wilcoxon signed-rank test with multiple-testing correction

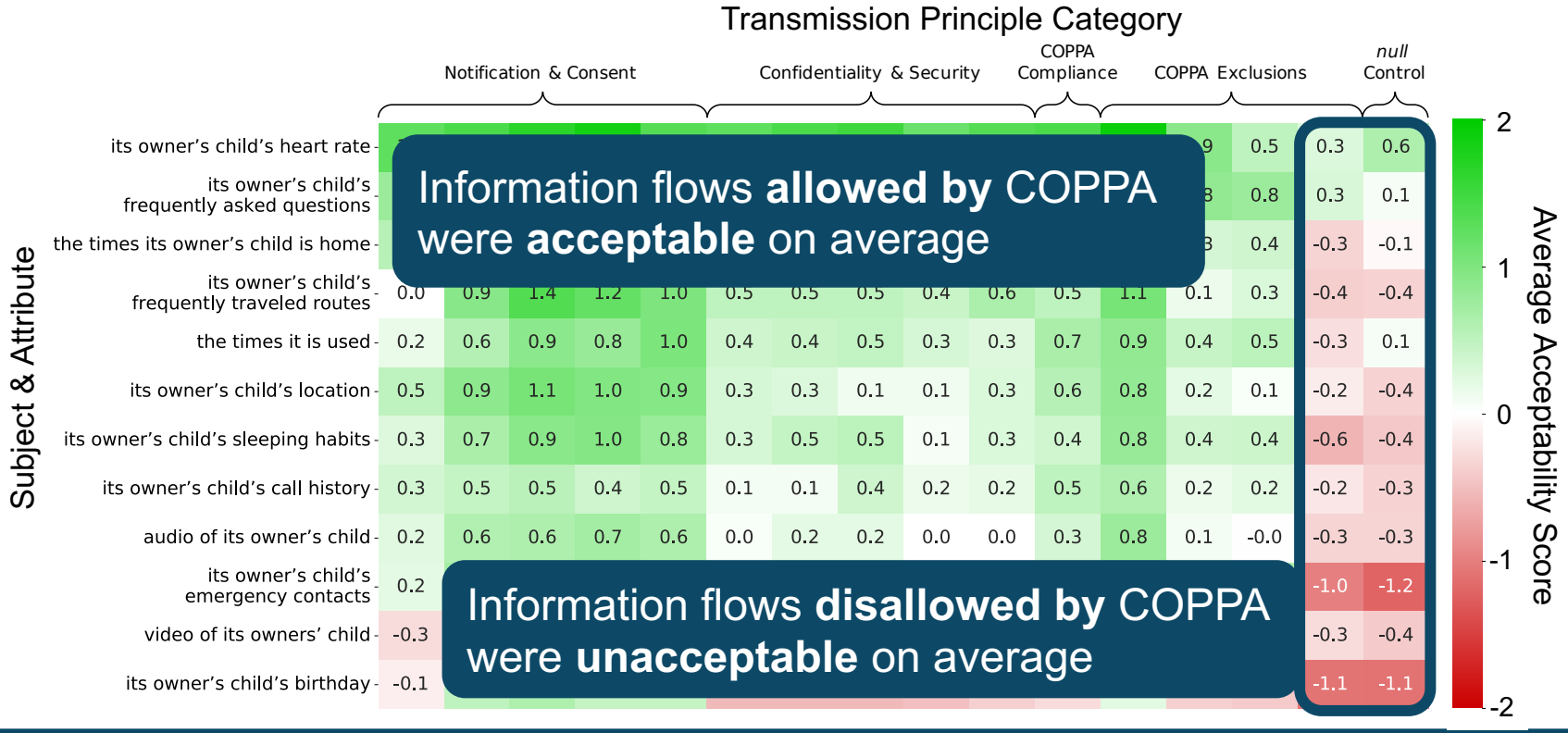
CI Survey Method Recap

1. Choose parameter values from regulation (COPPA)
2. Generate questions about acceptability of 1056 5-parameter information flows
3. Test survey with cognitive interviews
4. Deploy survey to 195 U.S. parents of children ages 3-13
5. Group responses by parameter & demographics
6. Compare acceptability scores across groups

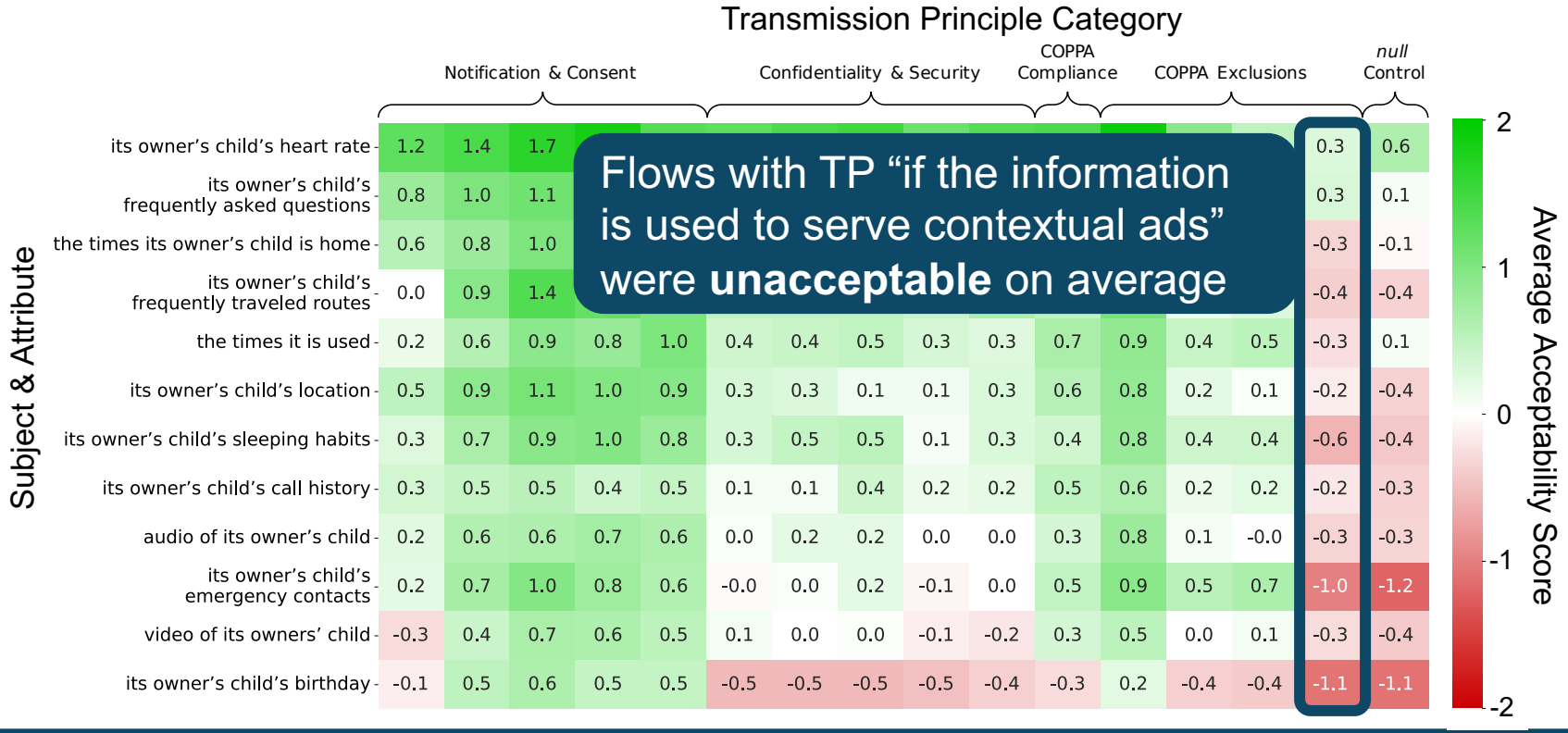
Results


Transmission Principle Category
Notification & Consent
Confidentiality & Security
COPPA Compliance
COPPA Exclusions
null Control
Subject & Attribute
its owner's child's heart rate 1.2 1.4 1.7 1.8 1.3 1.2 1.4 1.5 1.2 1.3 1.4 1.9 0.9 0.5 0.3 0.6
its owner's child's frequently asked questions 0.8 1.0 1.1 1.1 1.1 0.9 1.0 0.8 0.6 0.7 0.8 1.2 0.8 0.8 0.3 0.1
the times its owner's child is home 0.6 0.8 1.0 1.0 0.6 0.4 0.4 0.5 0.4 0.5 1.0 0.9 0.3 0.4 -0.3 -0.1
its owner's child's frequently traveled routes 0.0 0.9 1.4 1.2 1.0 0.5 0.5 0.5 0.4 0.6 0.5 1.1 0.1 0.3 -0.4 -0.4
the times it is used 0.2 0.6 0.9 0.8 1.0 0.4 0.4 0.5 0.3 0.3 0.7 0.9 0.4 0.5 -0.3 0.1
its owner's child's location 0.5 0.9 1.1 1.0 0.9 0.3 0.3 0.1 0.1 0.3 0.6 0.8 0.2 0.1 -0.2 -0.4
its owner's child's sleeping habits 0.3 0.7 0.9 1.0 0.8 0.3 0.5 0.5 0.1 0.3 0.4 0.8 0.4 0.4 -0.6 -0.4
its owner's child's call history 0.3 0.5 0.5 0.4 0.5 0.1 0.1 0.4 0.2 0.2 0.5 0.6 0.2 0.2 -0.2 -0.3
audio of its owner's child 0.2 0.6 0.6 0.7 0.6 0.0 0.2 0.2 0.0 0.0 0.3 0.8 0.1 -0.0 -0.3 -0.3
its owner's child's emergency contacts 0.2 0.7 1.0 0.8 0.6 -0.0 0.0 0.2 -0.1 0.0 0.5 0.9 0.5 0.7 -1.0 -1.2
video of its owners' child -0.3 0.4 0.7 0.6 0.5 0.1 0.0 0.0 -0.1 -0.2 0.3 0.5 0.0 0.1 -0.3 -0.4
its owner's child's birthday -0.1 0.5 0.6 0.5 0.5 -0.5 -0.5 -0.5 -0.5 -0.4 -0.3 0.2 -0.4 -0.4 -1.1 -1.1
Average Acceptability Score
2
1
0
-1
-2

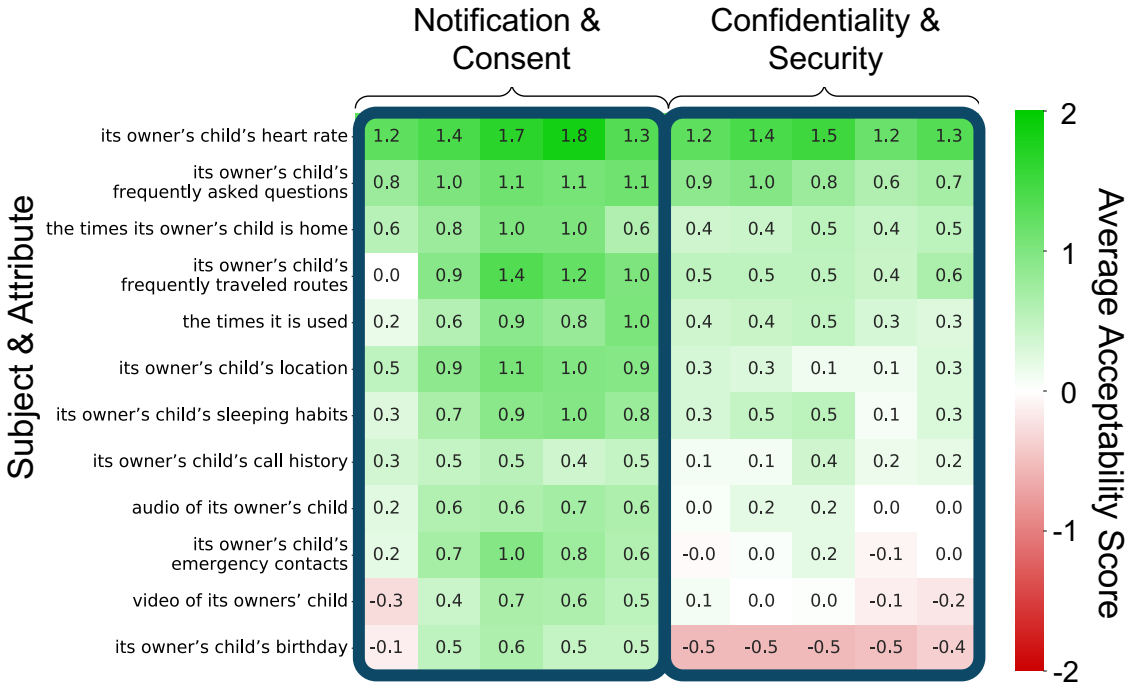
Parents' Norms Align with COPPA



Parents Dislike Targeted Ads

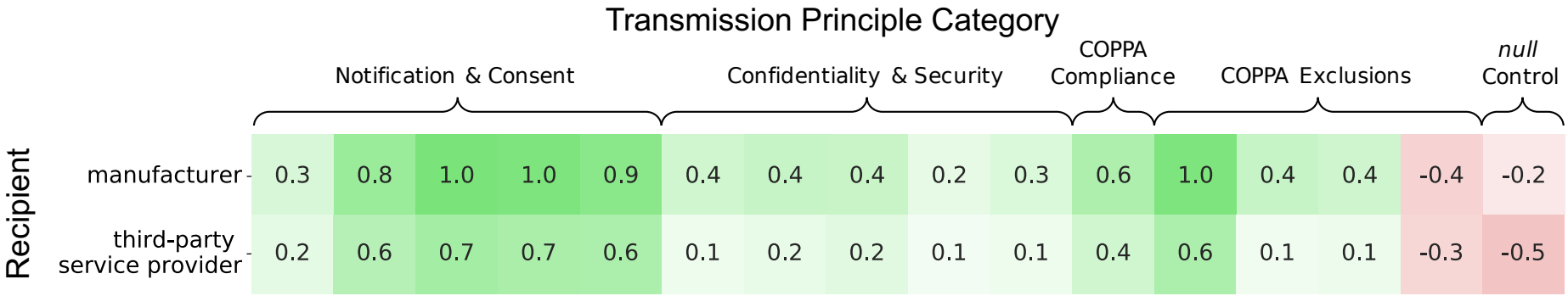


Notification & Consent are More Influential than Confidentiality & Security



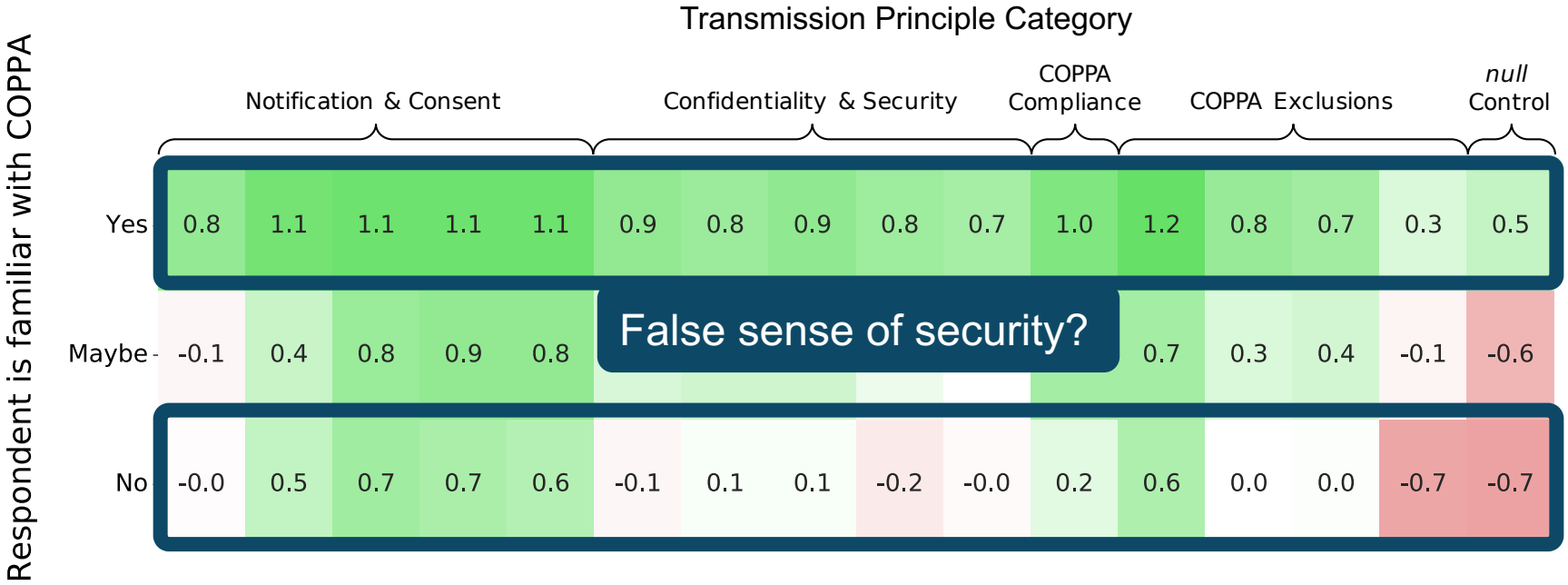
BUT… existing consent mechanisms (esp. privacy policies) are ineffective

Data Collection by Manufacturers is More Acceptable than by Third Parties

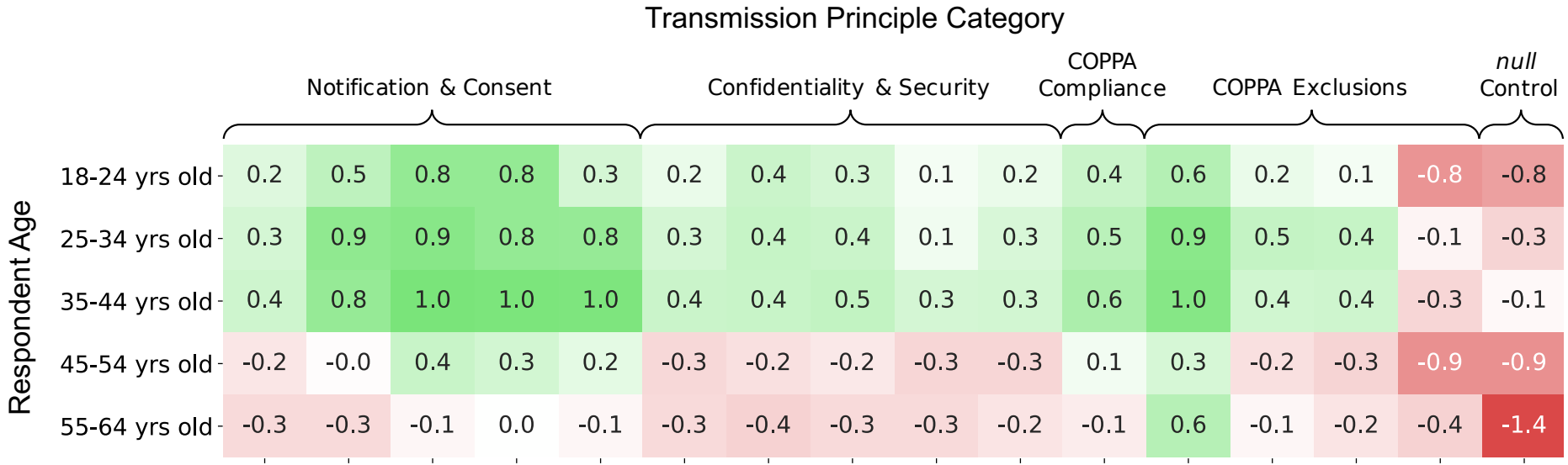


- COPPA only distinguishes between first- & third-parties
- Parents' privacy norms may vary between more specific recipients

Parents Familiar with COPPA View Data Collection as More Acceptable



Older Parents View Data Collection as Less Acceptable



Results Recap

- Parents' privacy norms generally align with COPPA
- Parents' dislike targeted ads
- Notification & consent are more influential than confidentiality & security
- Data collection by manufacturers is more acceptable than by third parties
- Parents familiar with COPPA view data collection as more acceptable
- Older parents view data collection as less acceptable

Future Work

- CI survey method → Other privacy regulations
  - HIPAA, FERPA, GDPR, CalOPPA
- Surveys about draft regulation → Informed policymaking
  - Also applicable to system/application design
- Longitudinal surveys → Norm changes over time
  - Does regulation affect norm evolution?

Conclusions

- We used a CI survey to compare COPPA to parents' privacy norms
- We found that COPPA data handling requirements significantly increase information flow acceptability
- Untested contextual factors & technical specifications not currently in COPPA may impact privacy opinions...and enforcement matters!

https://www.cs.princeton.edu/~apthorpe/