RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SEM-M01

Rethinking Access Control and Authentication for the Home IoT

Blase Ur

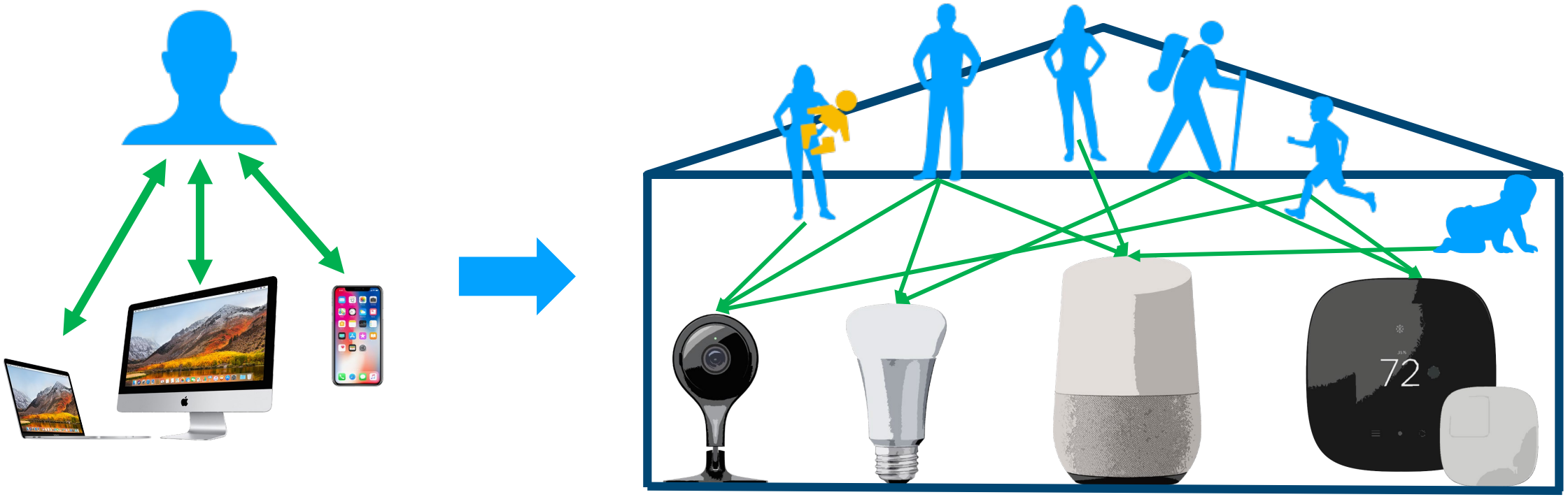
Neubauer Family Assistant Professor
Department of Computer Science
University of Chicago


c|net
CNET Smart Apartment - cnet.com

From Single User to Multi User

Single User

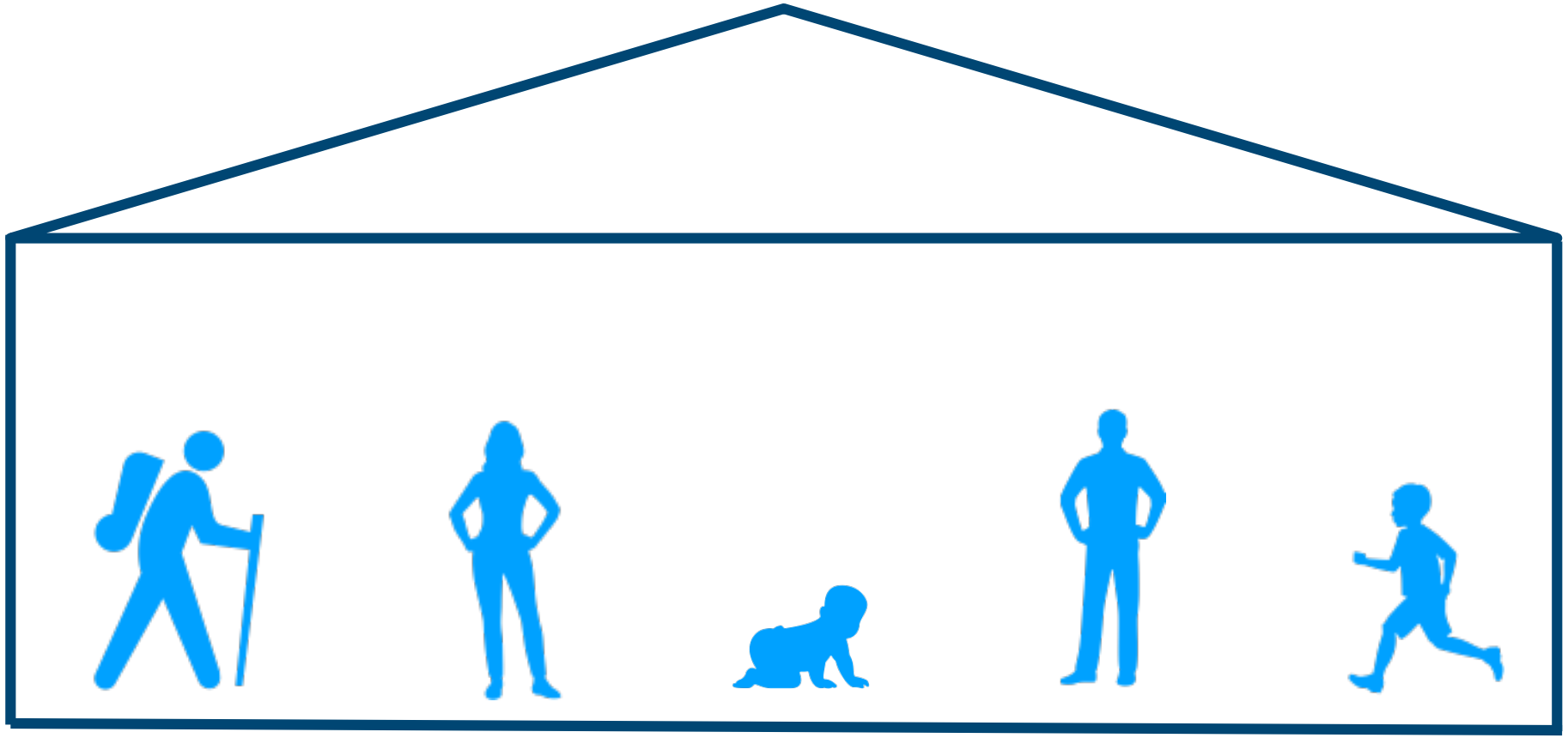
From Single User to Multi User



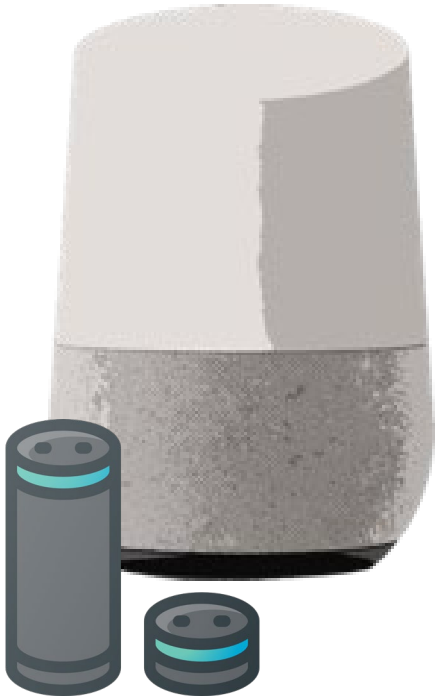
Single User

Multi User

Users Have Complex Social Relationships



Capabilities Have Different Sensitivities



The Absence of Screens and Keyboards

Research Goals

We conducted a user study to…

- Map desired access-control policies for home IoT devices
  - How policies vary by relationships and capabilities
  - Identify potential default policies

RSAConference2019

Method

User Study

Imagine you are the owner of a <smart device>.

Using this device, some users can access the following feature:

<capability>

6x **When should <relationship> be able to use this feature?**

- Always
- Sometimes
- Never

User Study

Imagine you are the owner of a Smart Voice Assistant.

Using this device, some users can access the following feature:

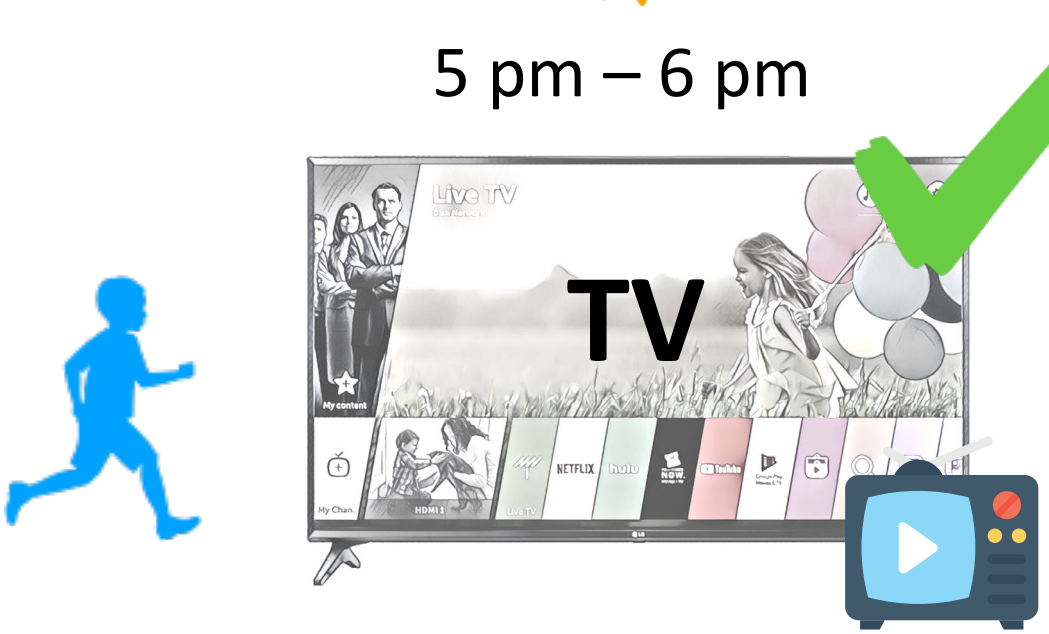
Make online purchases (e. g., on Amazon) on a shared household account

When should your spouse be able to use this feature?

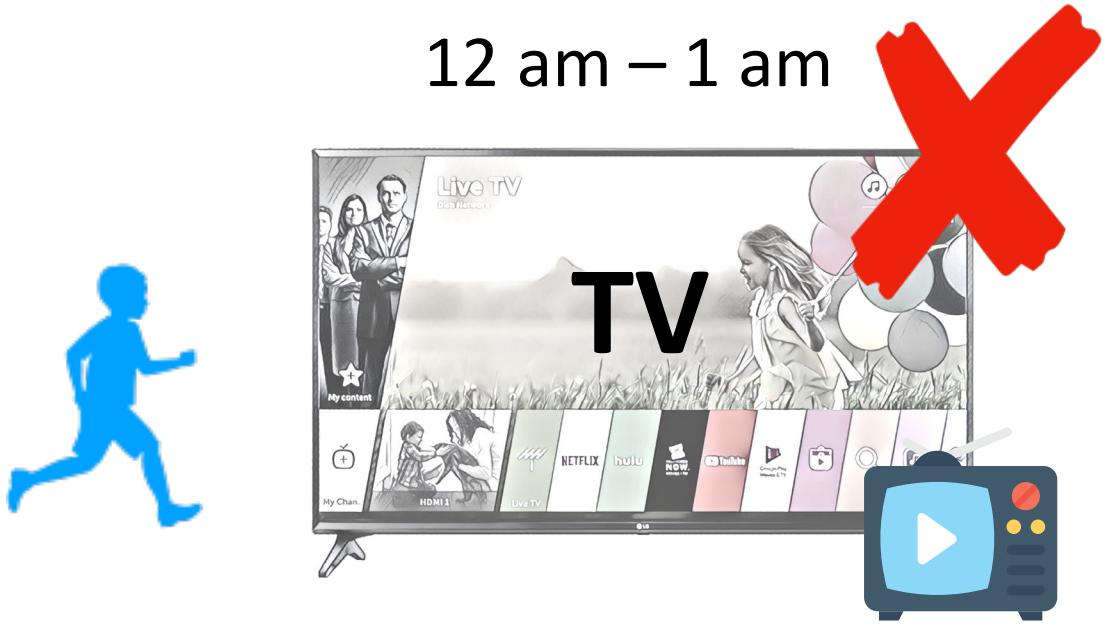
- Always
- Sometimes
- Never

Are Relationships and Capabilities Enough?

5 pm – 6 pm



12 am – 1 am



Research Goals

We conducted a user study to…

- Map desired access-control policies for Home IoT Devices
  - How policies vary by relationships and capabilities
  - Identify potential default policies
- What contextual factors affect the user's decision?

6 Relationships

24 Relationships

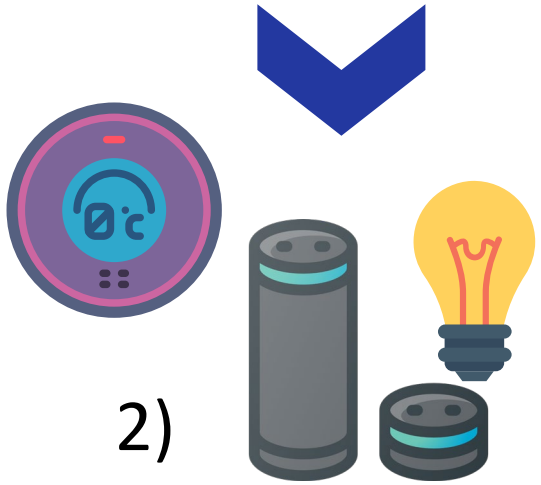
6 Relationships

- Your Spouse
- Your Teenage Child
- Your Child in Elementary School
- A Visiting Family Member
- The Babysitter
- Your Neighbor

22 Capabilities

1)

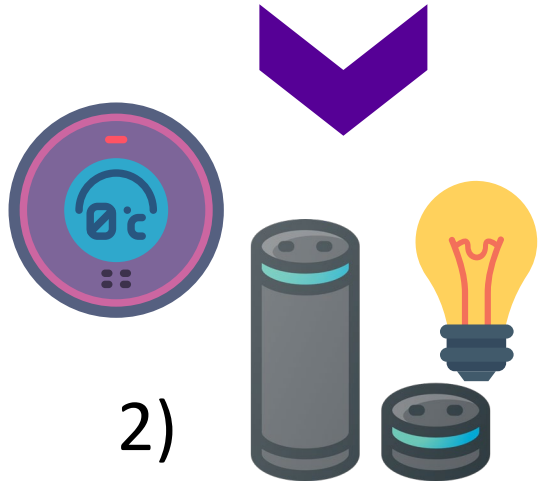
2)



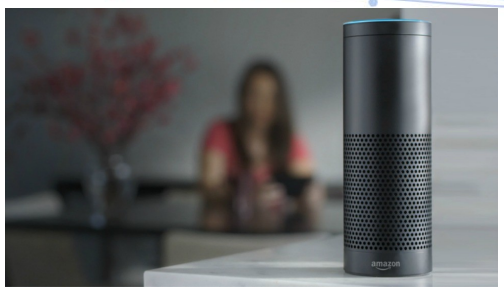
22 Capabilities

1)

2)



3)

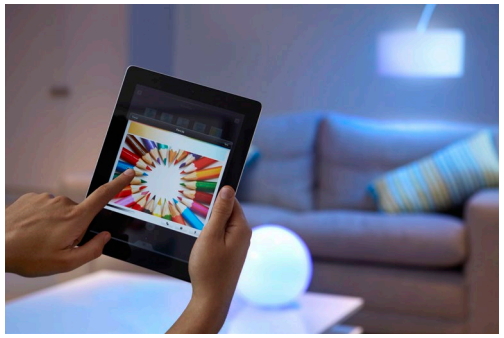


Order Online

Live Video

Answer Door

Mower (Rule)



Lights (Rule)

Alexa - amazon.com, Nest Cam - nest.com, Ring Doorbell - thewirecutter.com, Husqvarna Automower - husqvarna.com, Hue - philips.com

RSAConference2019

Results

425 Participants

54% Male

46% Female

Age

25-34

47%

CS

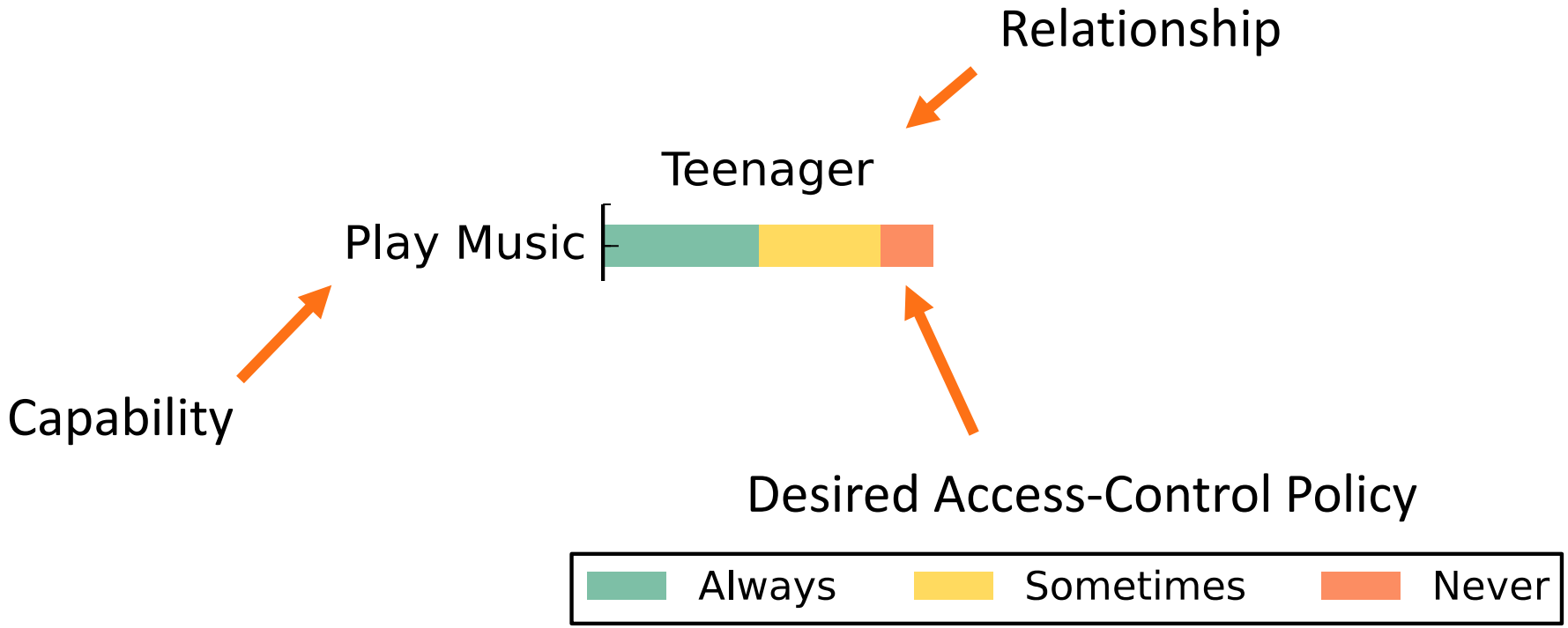
19%

Home IoT Device

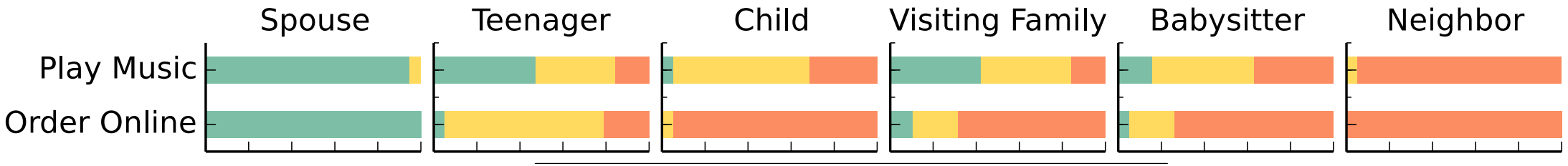
44%

Results

- Given one particular capability, what access-control policy should be set up for whom?



Comparison Between Capabilities

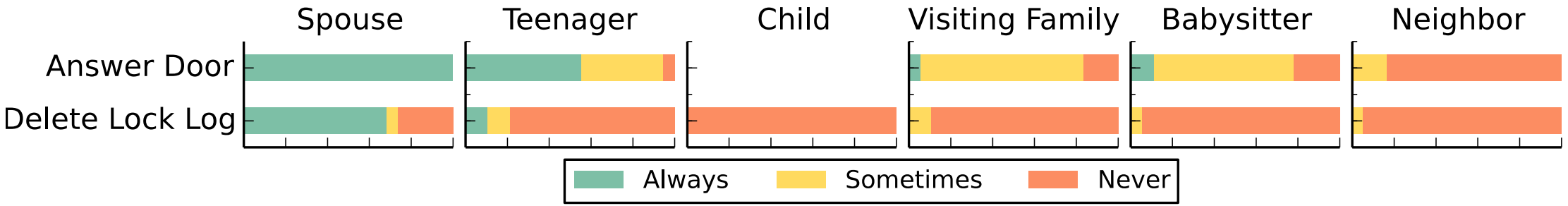


Icon made by Alexander Madyankin, Roman Shamin, Echo Plus with built-in Hub – Black - www.amazon.com

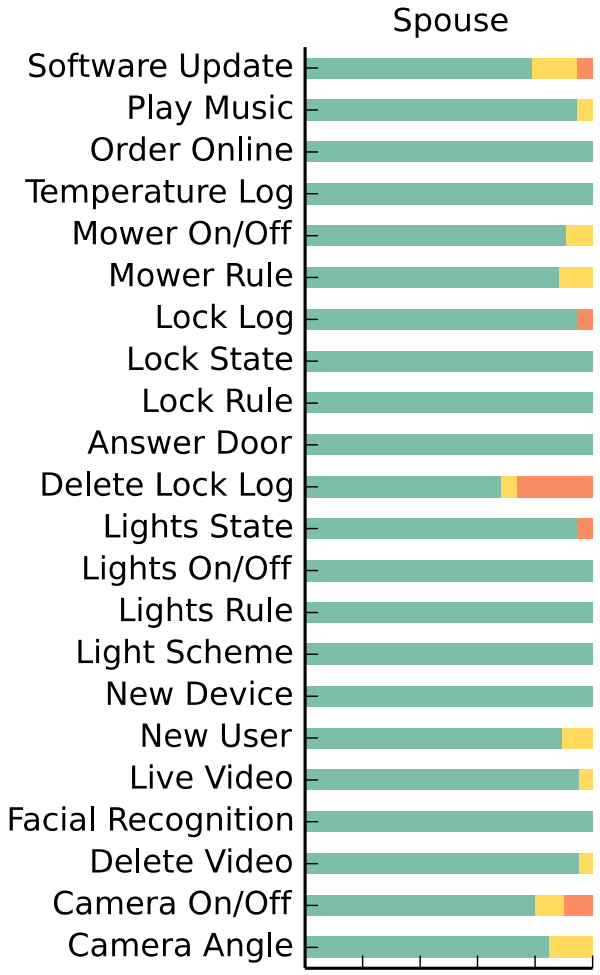
Capabilities Within One Device

Answer Doorbell

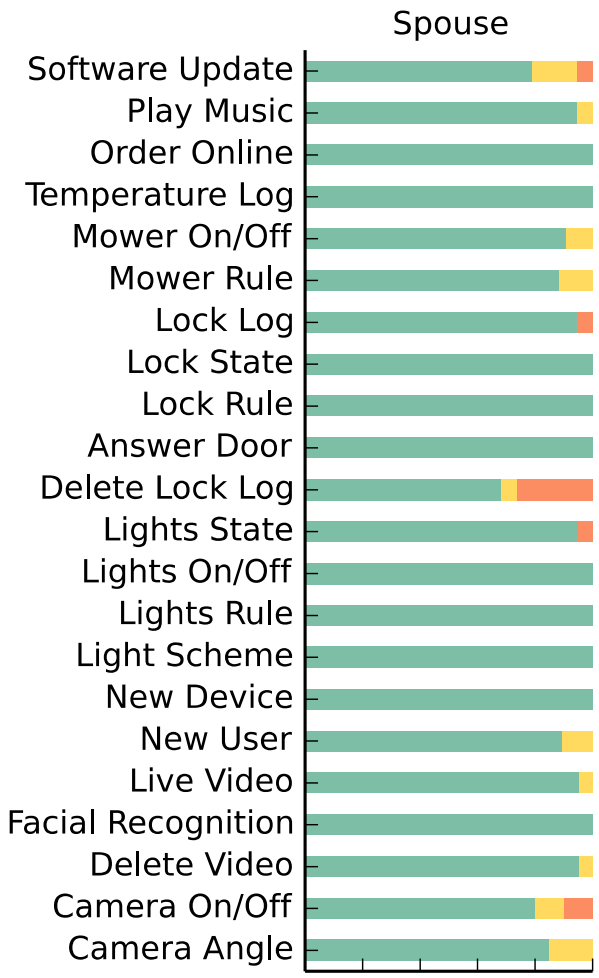
Delete Lock Log

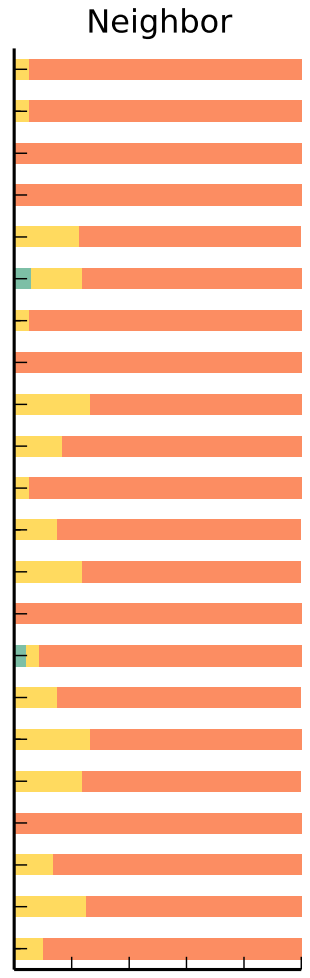


Spouse Can Do Almost Everything

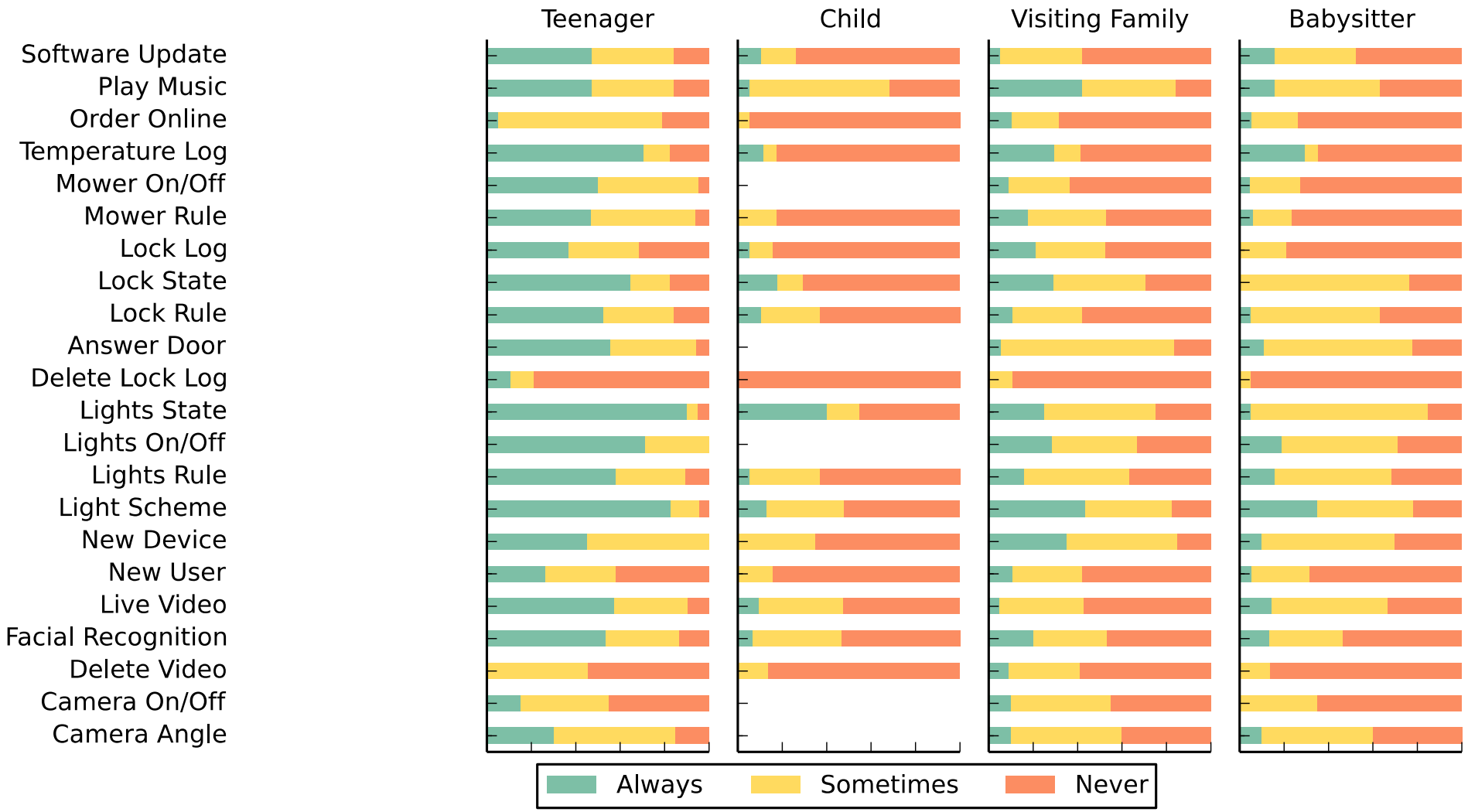


Neighbor Can Do Nothing





Other Relationships Are More Complex



Relationships Matter…But Are Not Enough

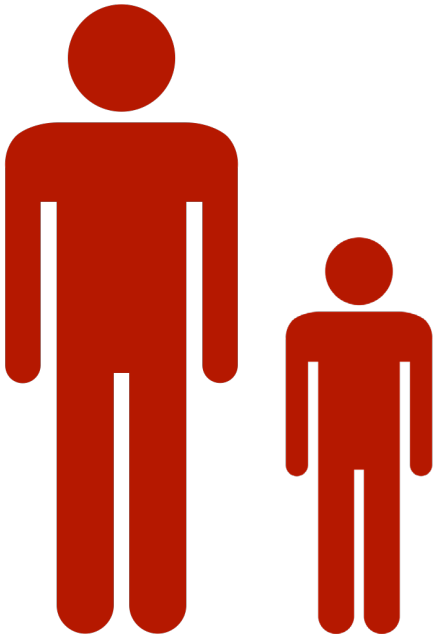
Relationships Matter…But Are Not Enough

What does *sometimes* mean?

RSAConference2019

Contextual Factors

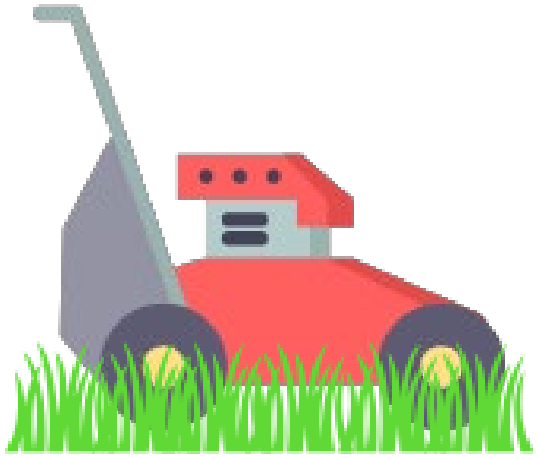
Factor: People Around



Child

"They would be allowed to use it whenever I am home with them."

Factor: Time of Day



"I would not want anyone trying to use the mower at night. The neighbors would most likely get mad."

Factor: Location of User

"Why do you need to use it if you aren't close?"

Factor: Location of Device

"If it is used in the bedroom then it would matter who has access."

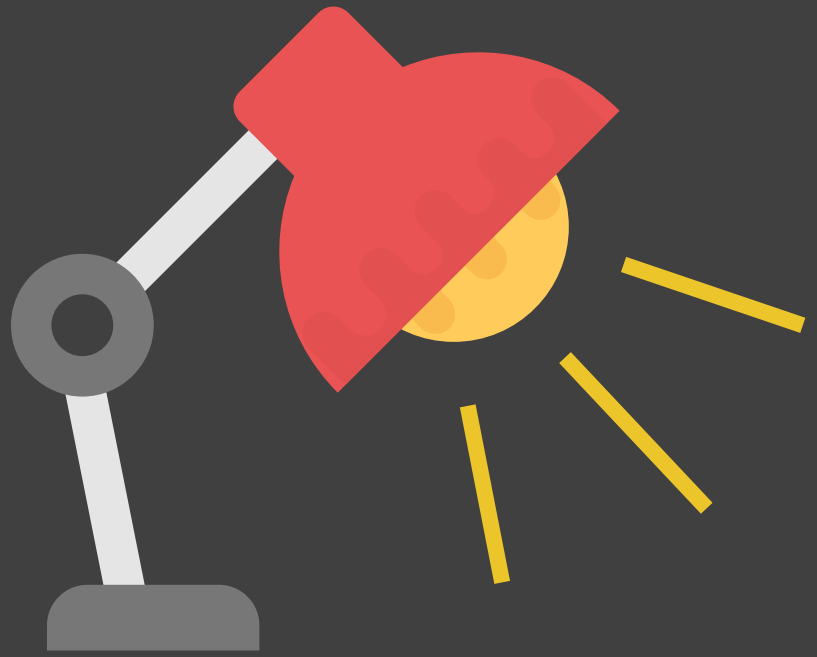
bedroom-21 - ffooty.com

Factor: Explicit Permission

"When they are authorized by the owner."

Factor: Consequences

Factor: Responsible Usage



“They shouldn't use the lights if they are using them too frequently.”

Recap: Missing From Current Systems

Relationships

Capabilities

Contextual Factors

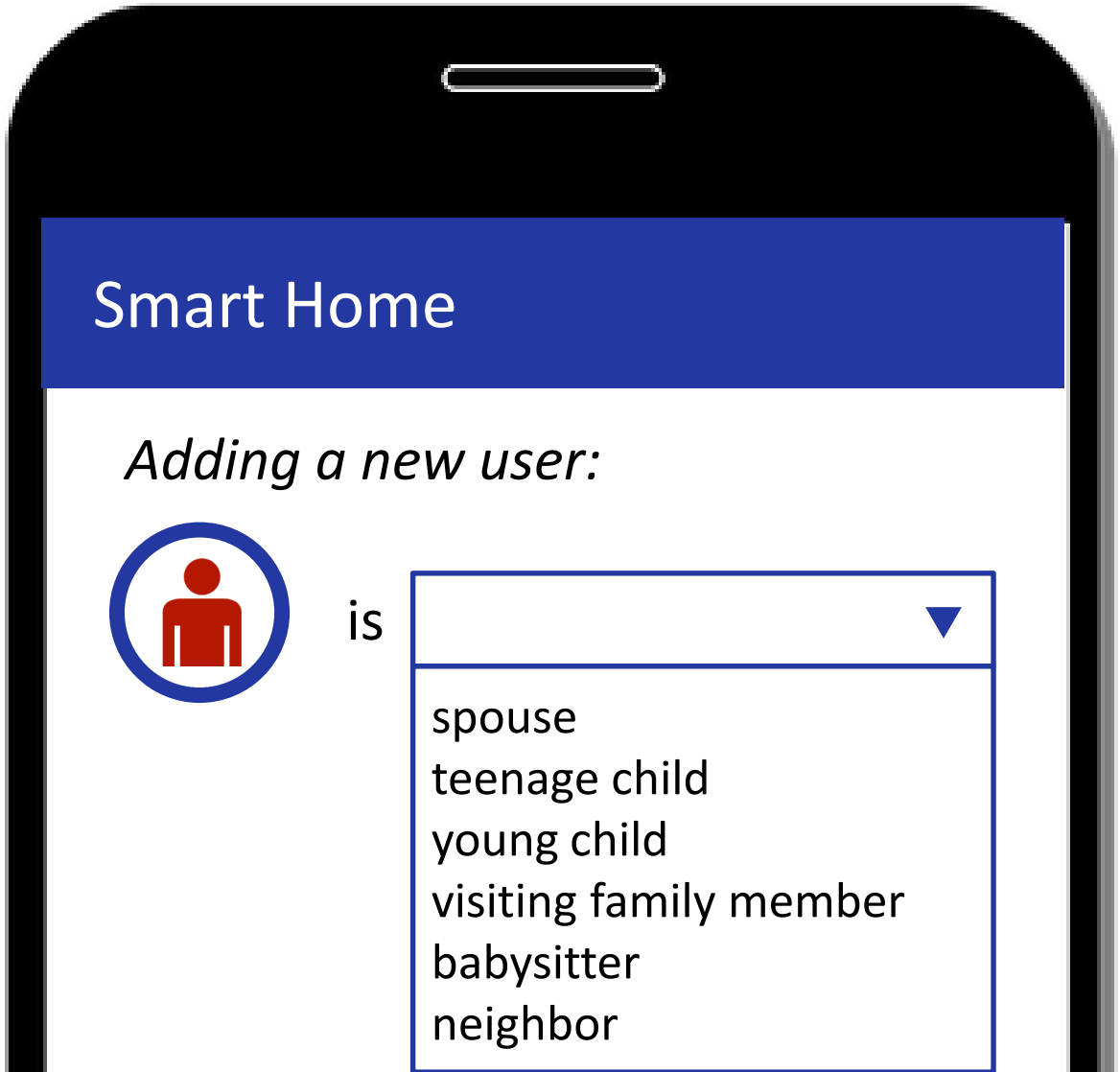
RSAConference2019

Design Implications

Current: Guest vs. Owner

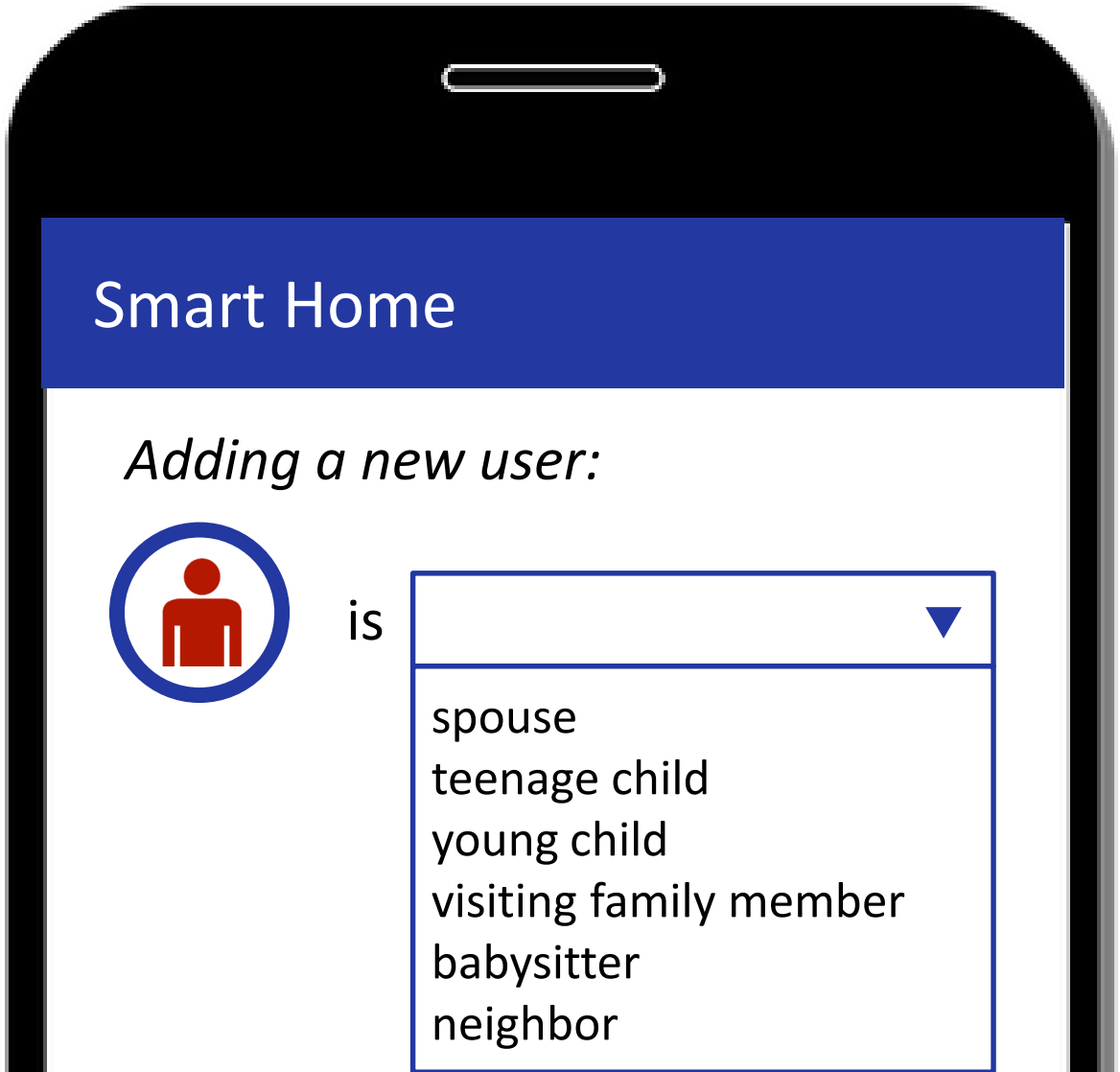
Smartphone Icon – pixabay.com

Future: Designing for Relationships



Smartphone Icon – pixabay.com

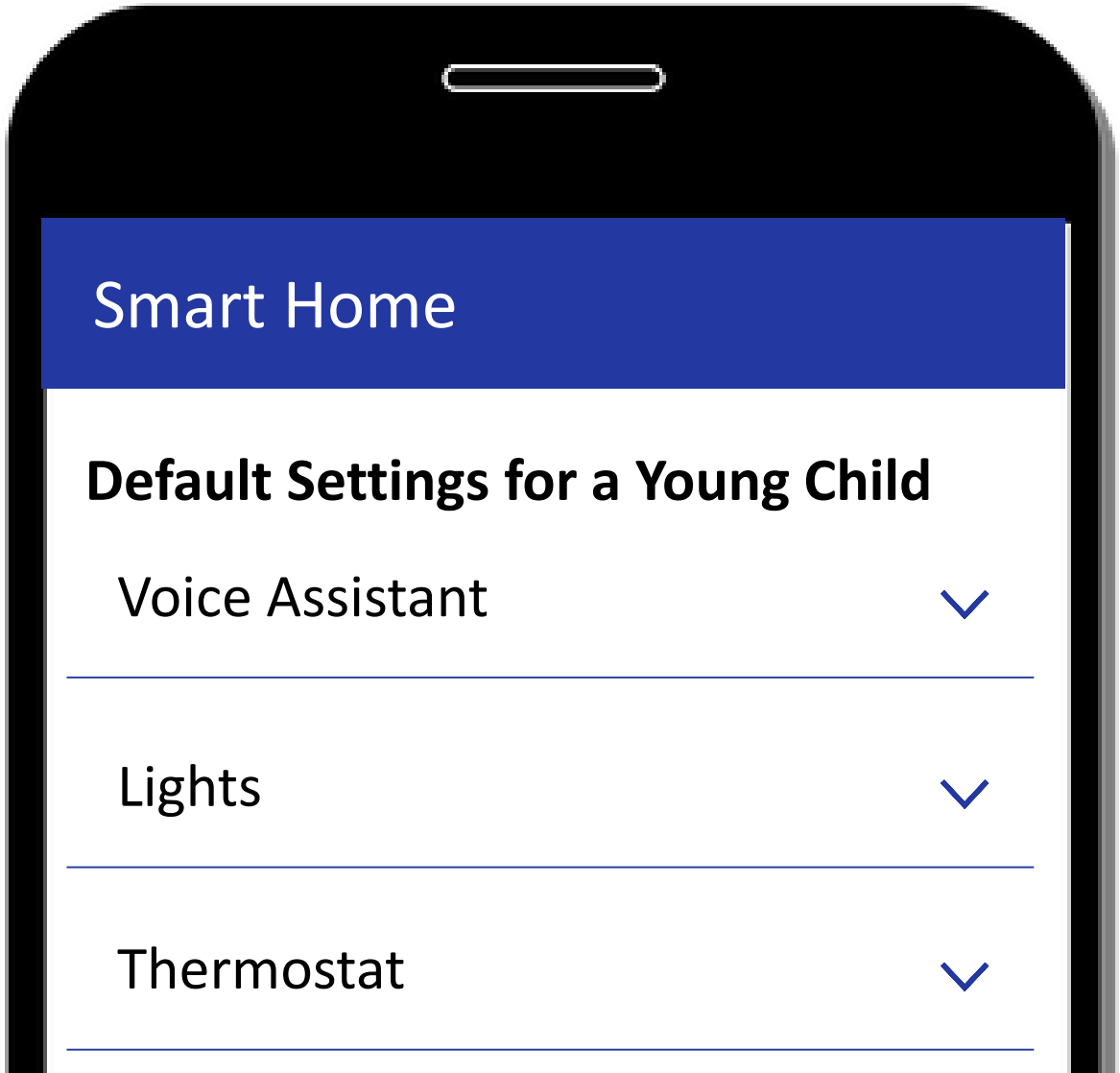
Future: Designing for Relationships



Smartphone Icon – pixabay.com

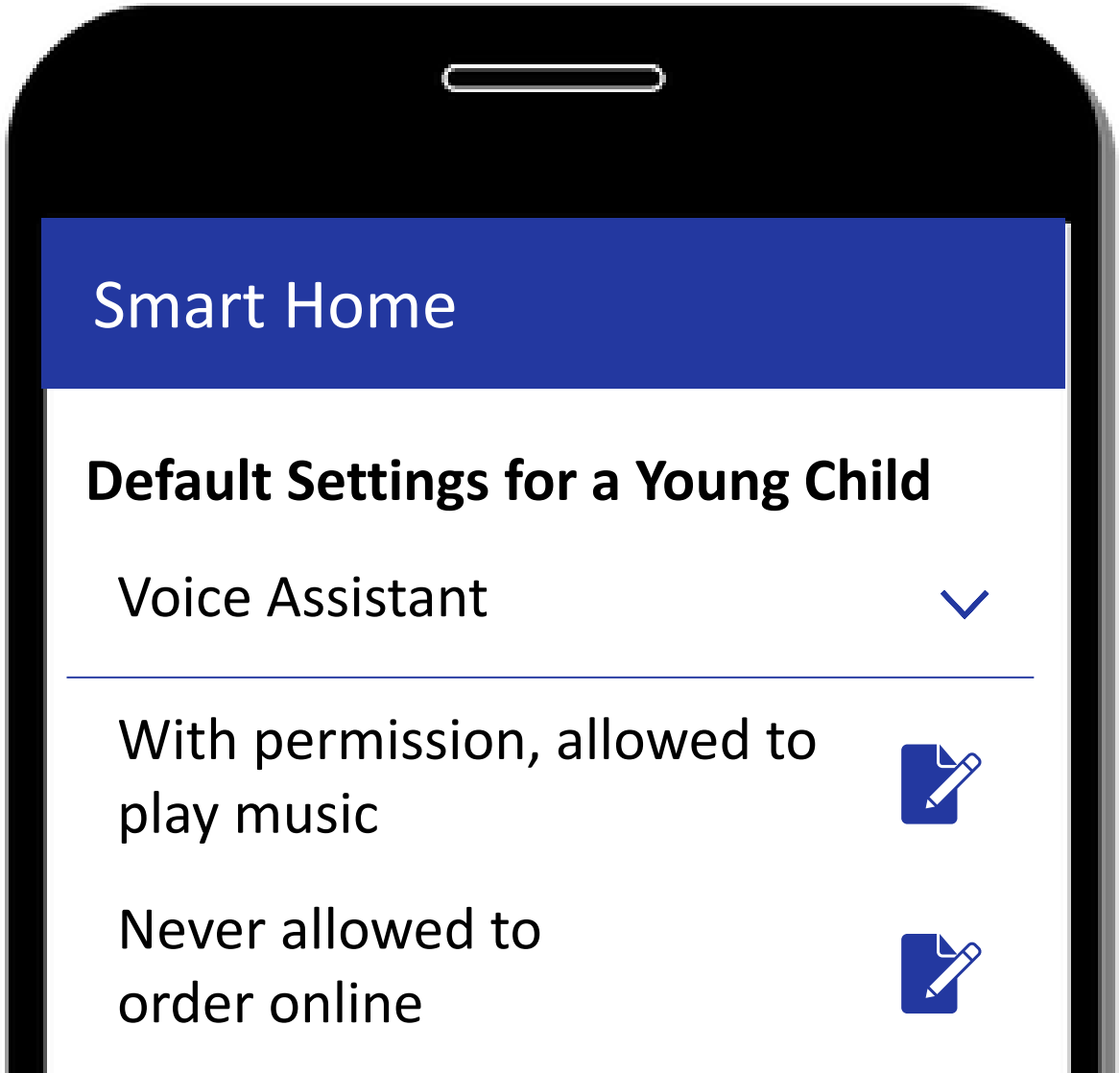
Future: Designing for Relationships

Future: Relationships and Capabilities

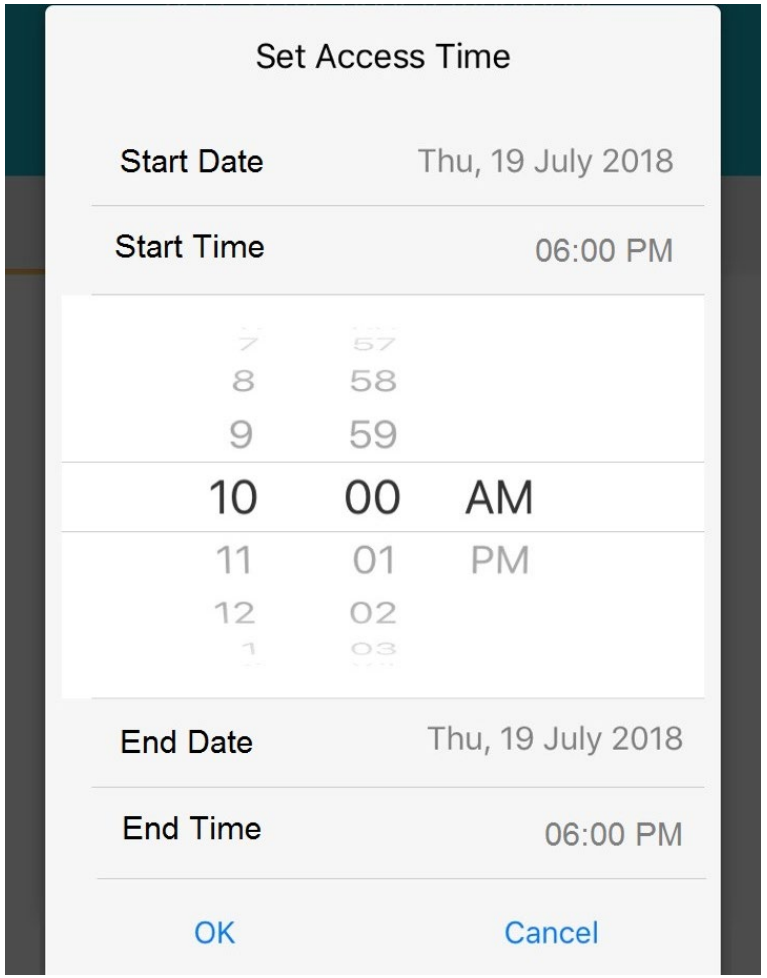


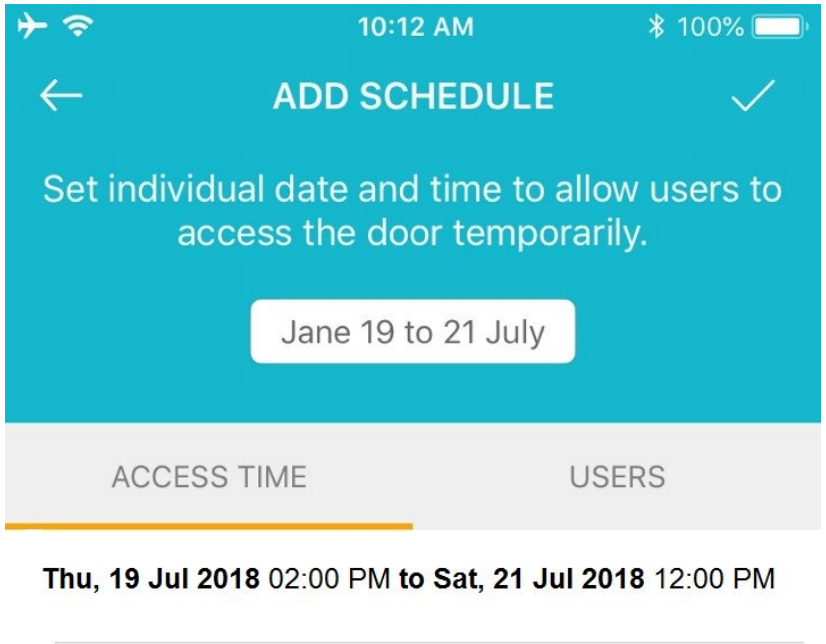
Smartphone Icon – pixabay.com

Future: Relationships and Capabilities



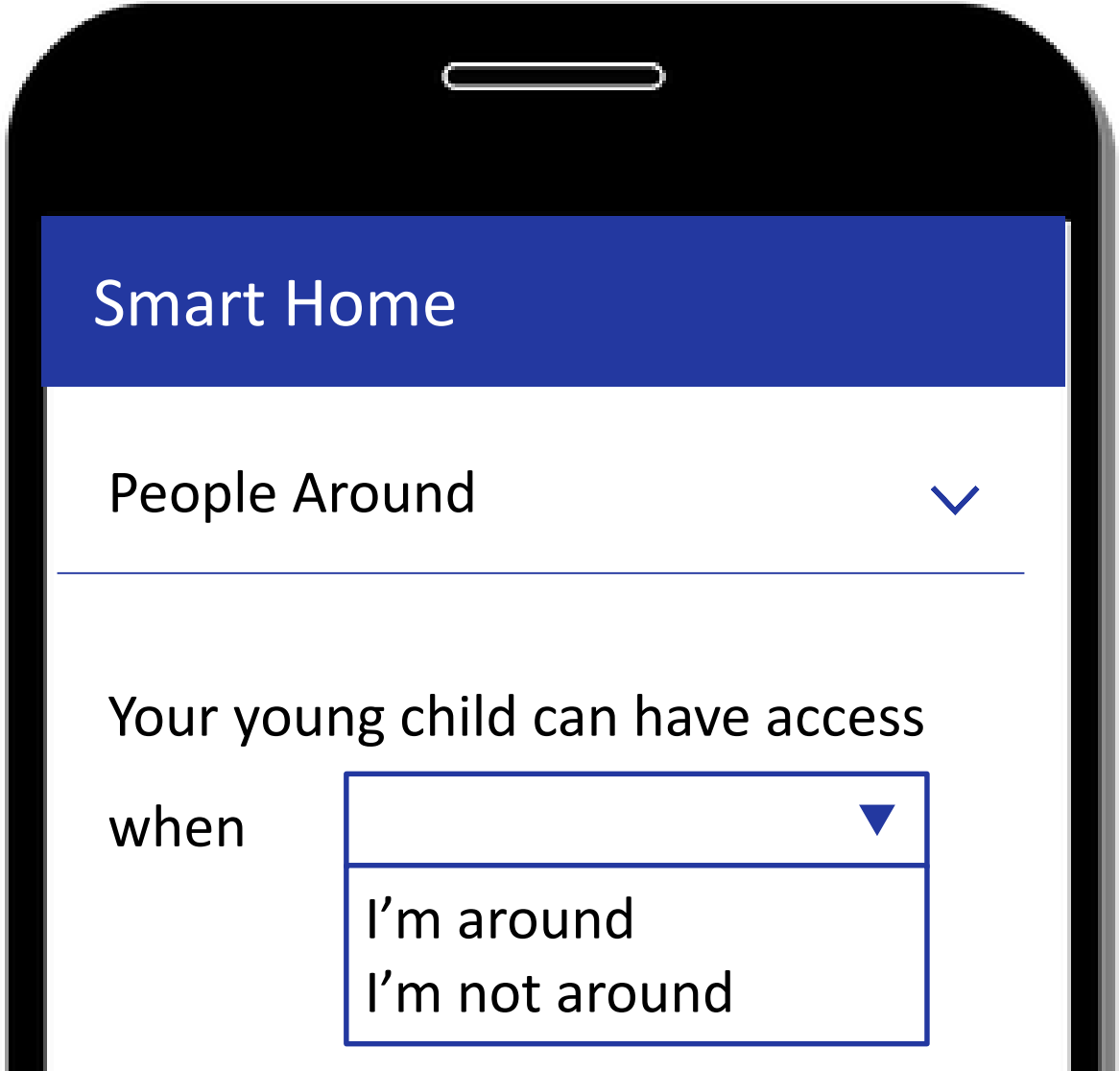
Current: Full Access or Temporary Access





TimeTec Admin Guide-Airbnb with Smart Lock - www.timetecsecurity.com/

Future: Contextual Factors



Smartphone Icon – pixabay.com

RSAConference2019

Capability-Based Access Control

Relationships → Default Policies

Support Context-Dependent Policies

Rethinking Access Control and Authentication for the Home IoT

Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, Blase Ur

THE UNIVERSITY OF CHICAGO

RUHR UNIVERSITÄT BOCHUM RUB

UNIVERSITY of WASHINGTON