

# Security & Privacy at Home



**Blase Ur, Ph.D. Candidate, CMU**

# Traditional UPS Issues at Home

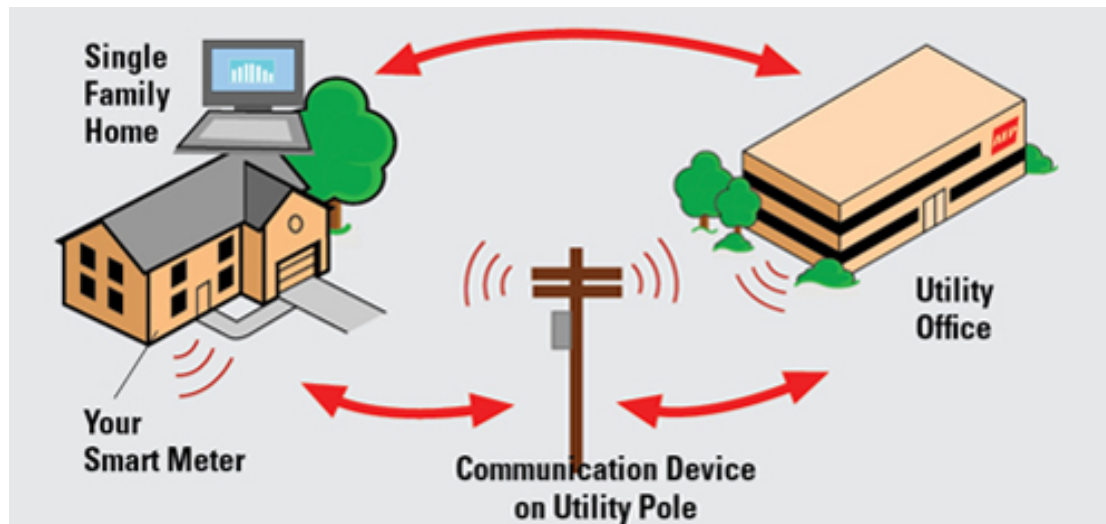
- Sharing and protecting data in the home
  - Heterogeneous set of (related) users
  - Many devices
  - Lots of sensitive data
- Controlling access to home wi-fi networks
- Device pairing based on location-limited channels

# Privacy in the Home

- The home traditionally is considered private (e.g., Warren and Brandeis Harvard Law Review Article)
  - “The right to be let alone”
  - Domestic life is a “sacred precinct”
  - But is the home really private?

# Smart Homes and the Internet of Things

- Network everything!
  - Sensors around the house and carried by the user
  - Smart (energy) meters
  - Household appliances
  - Cars
  - Healthcare devices



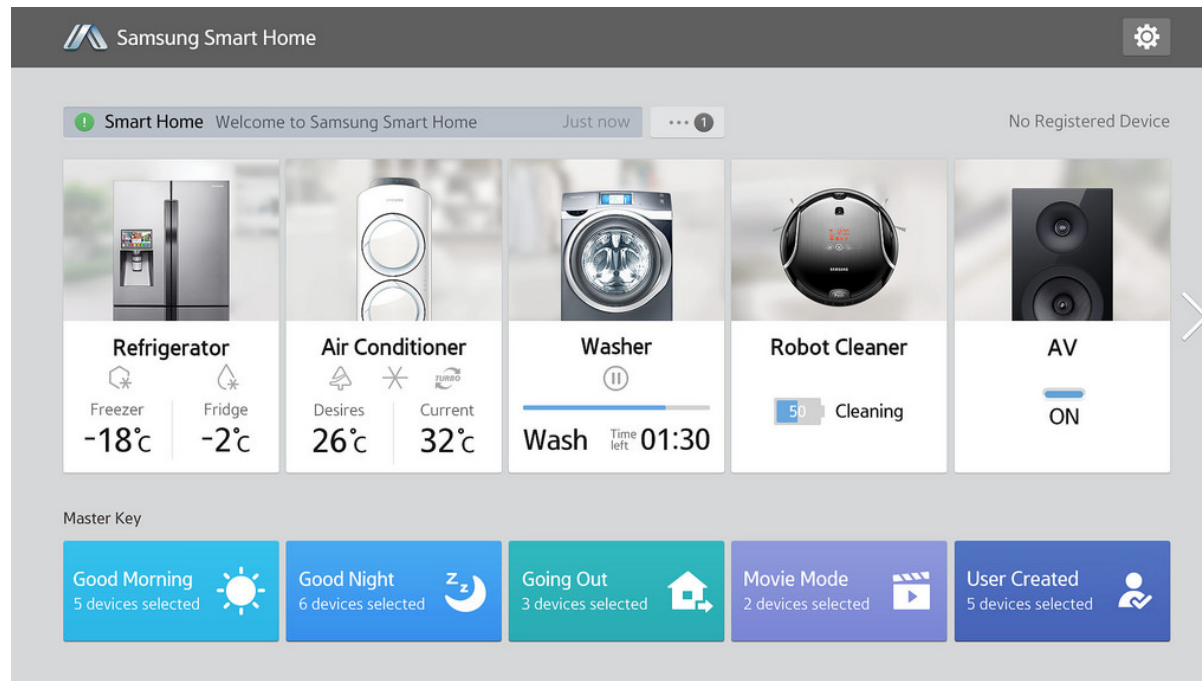






# Smart Homes and the Internet of Things

- Why network everything?
  - Convenience
  - Comfort
  - Customizability
  - Sustainability



# Privacy in the Smart Home

- To me, privacy at home is interesting because:
  - Home is traditionally a private space, but increasingly a window to the outside world
  - Heterogeneous occupants with complex power dynamics and perspectives
  - Visitors and guests
  - A large amount of time is spent there
  - Clear intentions for access control (and control considered more broadly)

# Privacy Threats in the Smart Home

- Surveillance by the government
- Surveillance by smart-home companies
- Surveillance by third-party security vendors
- Surveillance by Internet behemoths
- Surveillance by other members of the family
  - Parents → teens
  - Teens → parents
  - Spouse → spouse
  - Elder → younger
  - Younger → elder



# Privacy Threats in the Smart Home

- Direct data readings
- Inferences
  - What you are doing
  - What you are *not* doing
  - Incorrect inferences
- Loss of control (e.g., location tracking)
- Loss of autonomy (e.g., eldercare)
- Change of norms about private space
- Threats to security
- Threats to freedom of expression

# UbiComp '14 Study





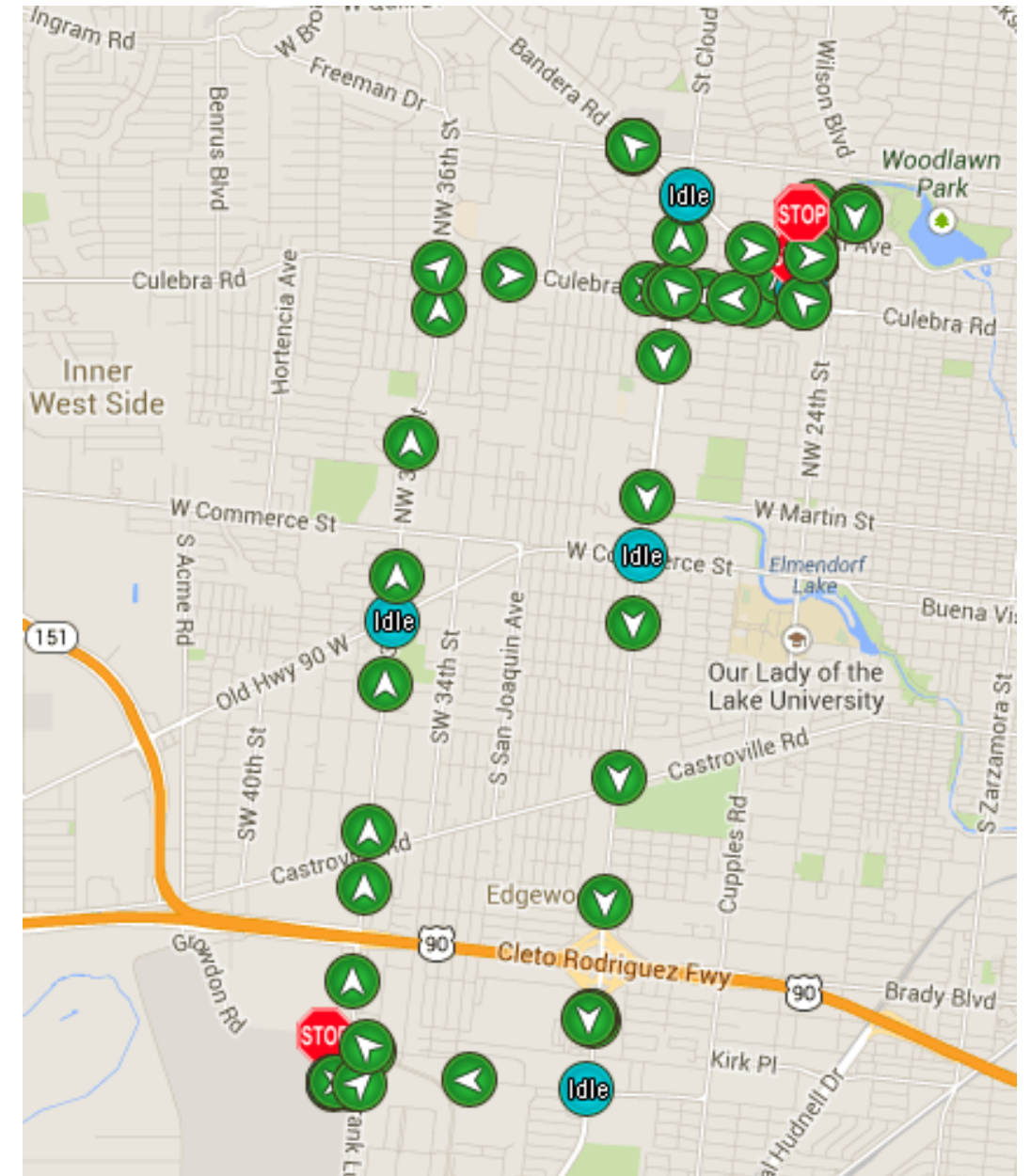
Photo taken by the authors.



# Home security



# Teen monitoring



# Home security and teen monitoring



**Gauge teenagers' and parents'  
reactions to Internet-connected  
locks and cameras  
in home entryways**

# Methodology

- Two studies:
  - Interviews of parents and teenagers
  - Online configuration study

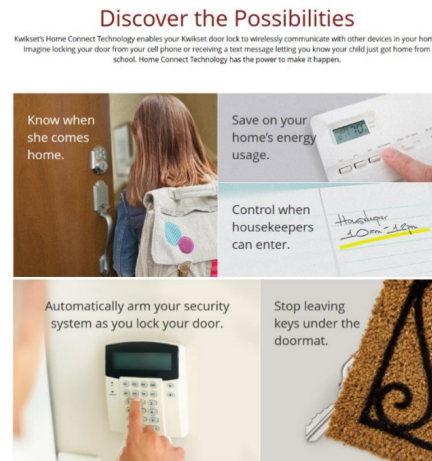
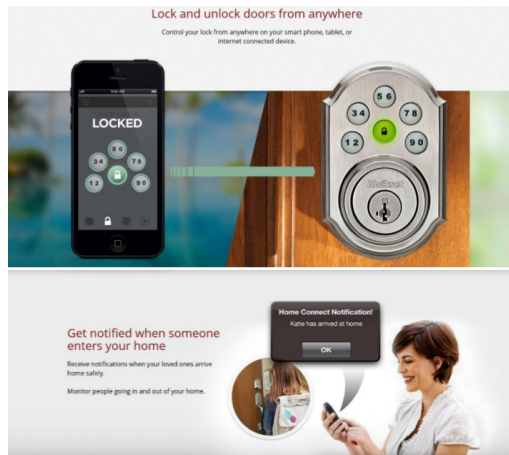


# Interview Study Methodology

- Interviewed 13 teenagers and 11 parents
  - Recruited from Microsoft's participant pool
  - All from different households
  - Limitation: Not a representative sample
  - Limitation: Hypothetical deployment
- Interviews lasted ~1 hour
  - Compensation: \$50 gift card or equivalent

# Interview Structure

- Parenting-style survey
- Familiarity with, and use of, home technology



- General reactions to Internet-connected locks
- Use of traditional keys and history of burglaries
- Reactions to potential interfaces for audit logs
- Current monitoring practices and attitudes

# Analysis

- Transcribed all interviews
  - Two researchers tagged 1,852 quotes as explanatory
- Collaboratively performed affinity diagramming
  - Identified 28 primary themes representing attitudes and influences

# Participants

- 13 teenagers (7 male, 6 female)
  - Age 15 – 17
  - Range of family circumstances
- 11 parents (4 male, 7 female)
  - Age 35 – 59
  - Two single parents
  - One parent uses an Internet-connected lock





# Participants Liked Connected Locks

- Parents and teens said there were substantial benefits in Internet-connected locks
- Benefits include:
  - Convenience
  - Added control
  - Safety from burglars
- Drawbacks are:
  - High cost
  - Fear of hackers

# Auditing Interfaces




# Auditing Interfaces

## Photo log

What?	How? / Who?	When?
Rear door 		19 minutes ago
Rear door 	Aurora's Phone	20 minutes ago
Front door 		39 minutes ago
Front door 	Billy's PIN Code	40 minutes ago
Rear door 		4 hours ago
Rear door 	Billy's Phone	4 hours ago

# Auditing Interfaces

## Text log

<u>What?</u>	<u>How?</u>	<u>When?</u>
Rear door 	Aurora's Phone	20 minutes ago
Front door 	Billy's PIN Code	40 minutes ago
Rear door 	Billy's Phone	4 hours ago












# Auditing Interfaces

**No log**

# Parents' and Teens' Preferences Differed

- All 11 parents preferred photo log
  - “For safety purposes”
  - “You need to catch a burglar on camera”
- 3 specified monitoring teens as a goal
  - “As my son gets older, I’m going to need to verify if he’s coming home alone”

What?	How? / Who?	When?
Rear door 		19 minutes ago
Rear door 	Aurora's Phone	20 minutes ago
Front door 		39 minutes ago
Front door 	Billy's PIN Code	40 minutes ago
Rear door 		4 hours ago
Rear door 	Billy's Phone	4 hours ago

# Parents' and Teens' Preferences Differed

- 6 teens preferred photo log
  - 4 nonetheless expressed privacy concerns
  - “...kind of weird that they could just always look and see exactly who’s over.”
- 3 teens preferred text log
  - Photo “invasion of privacy, ‘big brother’ kind of thing”
- 4 teens preferred no log
  - Photo log “would pretty much ruin a strict parent’s kid’s social life.”
  - “This is like parents going psycho.”

# Monitoring Teens

- Some parents wanted to monitor teens
  - “Trust but verify”
- Others chose photo log in spite of monitoring
  - “It’s just a human nature thing that nobody likes when people keep tabs on anybody”
  - “I think [my children] would be paranoid or intimidated by the photos”

# Current Monitoring Practices

- Unconstrained monitoring (2 parents)
- No monitoring (3 parents)
  - “I’m just waiting to see if she gives me a reason not to let her just be free.”
- Intentionally limited monitoring (6 parents)
  - “I feel like that’s a violation of their privacy if I were to [log onto their Facebook]. I know that I have their permission, I know that I have the access, but that’s going further than I want to.”



# Parental Strictness vs. Auditing Decision

- Compared teens' parenting style survey results with decisions about audit log
- 5 of the 6 teens with comparatively stricter parents chose the photo log
- 1 of the 7 teens with comparatively less strict parents chose the photo log

# Potential Unintended Consequences

- Reduced parent-teen trust
  - Spend time at friends' houses instead
- Circumvention reducing security
  - Leaving doors unlocked and windows open
  - Removing window sensors
  - Disabling camera

**How might parents configure an auditable security system?**

# Methodology

- Online configuration study
  - Access & audit settings for entryway security system
- 19 parents recruited from classified ad sites
  - Compensated with \$15 gift card

# Configuration Task

## Users

First name or nickname	Email address or mobile phone #	Age	Lock PIN	Role	Lock and unlock records can be audited
<i>You, age 50</i>					
<input type="text" value="Alice"/>	<input type="text" value="alice@foo.com"/>	<input type="text" value="50"/>	<input type="text" value="••••"/>	<input type="text" value="administrator"/>	<input type="text" value="only with permission"/>
<i>Husband, age 53</i>					
<input type="text" value="Bob"/>	<input type="text" value="bob@foo.com"/>	<input type="text" value="53"/>	<input type="text" value="••••"/>	<input type="text" value="administrator"/>	<input type="text" value="anytime with notice"/>
<i>Daughter, age 16</i>					
<input type="text" value="Charlie"/>	<input type="text" value="202-555-9873"/>	<input type="text" value="16"/>	<input type="text" value="••••"/>	<input type="text" value="user"/>	<input type="text" value="anytime with notice"/>
<input type="text" value="Uncle Joe"/>	<input type="text" value="joe@foo.com"/>	<input type="text" value="40"/>	<input type="text" value=""/>	<input type="text" value="user"/>	<input type="text" value="anytime w/o notice"/>

## Notifications

Send a notification to  whenever   the door(s)

Email address or SMS phone #



# Configuration Task

The screenshot shows a configuration window titled "Configuration Task". At the top, there are input fields for "o.com", "50", a password field with four dots, "administrator", and a dropdown menu set to "only with permission". Below these fields is a text area containing the text: "You, and other auditors, can view records of when *Alice* locked or unlocked the door...".

There are three radio button options for record access:

- ☒ **Only with permission from *Alice***  
*Alice* will be sent a text or email asking him/her to approve the release of these records.
- ☐ **Anytime, but a notification will be sent to *Alice***  
*Alice* will receive a text or email indicating who accessed his/her records.
- ☐ **Anytime & without notice**  
*Alice* will not be notified when his/her records are accessed, but will know who can access them.

Below the radio buttons is a "save" button. Further down, there is a text area with the text: "*Alice* will be able to see which policy has been assigned to him/her and which users can read his/her lock and unlock records." Below this is another text area with the text: "Records of lock and unlock events are protected by the policy in place at the time of the event. Changing this policy will only change access to future lock and unlock events."

At the bottom, there is a dropdown menu set to "whenever", a text field containing "Charlie", and two buttons: "save" and "cancel". To the right of these buttons is a dropdown menu set to "the door(s)" and a button labeled "a".

At the very bottom of the window, there is a label "MS phone #".

# Results

- Most participants would only allow themselves to be audited with permission or with notice
- Participants assigned less privacy-protective settings for their spouses/partners
- All parents chose to monitor teens' comings and goings without notifying the teens
  - “She doesn’t have anything to hide, so it shouldn’t be a problem”
- Privacy is a negotiation between parents and teens

**How can we disentangle  
decisions about home security  
and teen monitoring?**

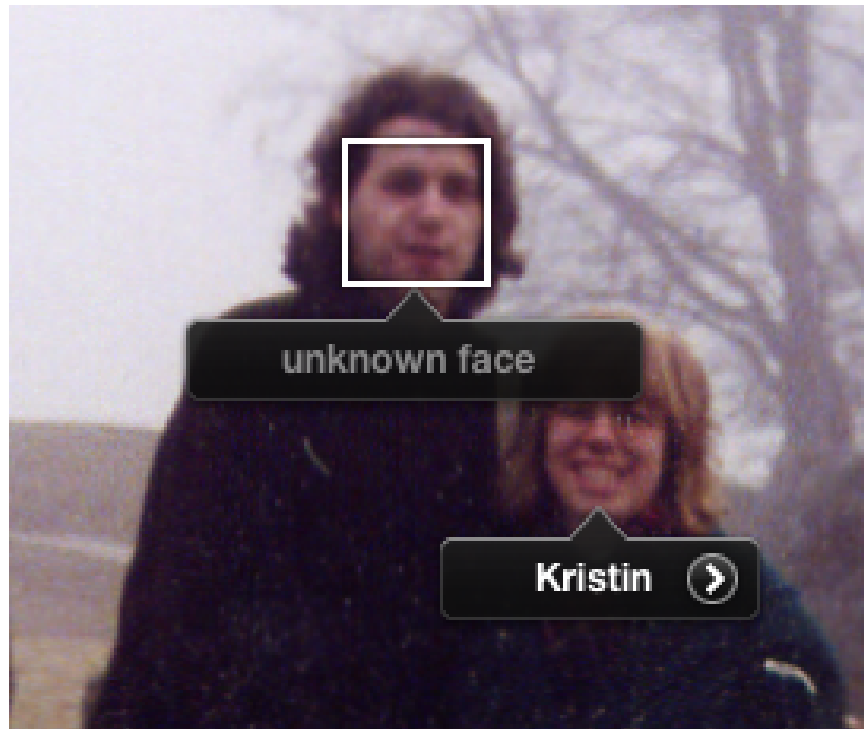
# Possible Directions

- “Outsource” auditing...
  - ...to a security company
  - ...to each individual



# Possible Directions

- Technology-assisted auditing
  - Face detection
  - Context-sensitive auditing



# Possible Directions

- Change the interaction with logs
  - Pull instead of push notifications
  - “Approximate” logs





# Conclusions

- New technologies can alter dynamics in the home
- Parents & teens had differing perspectives about audit
- Trust and security consequences result from conflating decisions about home security and teen monitoring
  - Potential interfaces and interactions that disentangle these decisions

# Future Directions in Smart-Home Research

- Mennicken et al.'s UbiComp '14 survey highlighted:
  - From augmented home to smart home
  - Meaningful technology
  - Working *with* technology
  - Intelligibility
- Why is intelligibility critical?
  - Debugging when things go wrong
  - Understanding the future
  - Engaging otherwise disenfranchised family members

# Future Directions in Smart-Home Research



# Future Directions in Smart-Home Research

- Intelligibility can leak private information
  - Imagine the Nest thermostat says, “I adjusted the temperature at 3:00am because people are always at the fridge then”
  - Imagine the smart meter says, “I noticed Johnny wastes energy all the time in his room”
  - Imagine Google shows you an ad for lightbulbs because “we noticed your kitchen is pretty dark”
- How do we support privacy as part of intelligibility?