

# Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance

Blase Ur  
Carnegie Mellon University\*  
bur@cmu.edu

Jaeyeon Jung  
Microsoft Research  
jjung@microsoft.com

Stuart Schechter  
Microsoft Research  
stus@microsoft.com

## ABSTRACT

We investigated how household deployment of Internet-connected locks and security cameras could impact teenagers' privacy. In interviews with 13 teenagers and 11 parents, we investigated reactions to audit logs of family members' comings and goings. All parents wanted audit logs with photographs, whereas most teenagers preferred text-only logs or no logs at all. We unpack these attitudes by examining participants' parenting philosophies, concerns, and current monitoring practices. In a follow-up online study, 19 parents configured an Internet-connected lock and camera system they thought might be deployed in their home. All 19 participants chose to monitor their children either through unrestricted access to logs or through real-time notifications of access. We discuss directions for auditing interfaces that could improve home security without impacting privacy.

## Author Keywords

Teenagers; parents; privacy; monitoring; audit mechanisms; domestic technologies; Internet of things (IoT); smart homes

## ACM Classification Keywords

H.1.2. User/Machine Systems: Human factors

## INTRODUCTION

Electronic locks and security cameras, already ubiquitous in workplaces, are increasingly being marketed for use in homes [12]. These systems promise convenience and peace of mind knowing that accesses are photographed. However, logs containing photographs can place everyone who lives in a home with such a system under surveillance, making them accountable to family members who have access to the logs. For instance, these logs could allow parents to monitor their teenagers' comings and goings, impacting the trust relationships and power dynamics between parents and teenagers. In effect, technologies installed for the safety of the whole household can have consequences for teenagers' privacy.

\*Work performed while at Microsoft Research.

Parents differ in their decisions about monitoring their children. Some parents require that teens give them their passwords or show them their text messages, whereas other parents actively choose not to do so in order to bolster parent-teen trust and encourage responsibility [18, 22, 26]. Previously, technologies that enabled parents to monitor their children were usually designed specifically for that purpose. For example, with parental controls on the computer [22, 27] and parental location-tracking software for phones [26], parents would decide whether to monitor their children based on their parenting style and the child's maturity. With the Internet-connected locks and cameras we investigate, however, the decision about whether to monitor teens is now conflated with decisions about protecting the security of the home.

We investigated the potential impact of Internet-connected locks and cameras on the balance between household security and teenagers' privacy. We first performed semi-structured interviews of 11 parents and 13 high school students. After discussing Internet-connected locks, we asked participants to choose between three options for auditing entries and exits: an interface with photos, a text-only interface, or no audit log.

While both teens and parents found benefits in Internet-connected locks, their preferences about auditability differed. Whereas all parents preferred audit logs with photographs, over half of the teens preferred text-only logs or no logs at all. Contrary to our expectations, five of the six teens who preferred logs with photographs rated their parents as comparatively most strict on a parenting-style survey.

We unpack these results by examining participants' parenting styles, experiences, and current practices. For instance, we examined why parents who did not currently monitor their teens' text messages or online accounts nonetheless chose the photo logs. These participants generally noted home security, rather than the ability to monitor their children, as their primary reason for choosing the photo log; surveilling their children was not a primary goal. We also identify consequences of the photo log, including reduced parent-teen trust and teen circumvention that would reduce the home's security.

To further investigate whether parents would voluntarily give teens privacy, we performed a follow-up online configuration study. A total of 19 parents living with teenagers configured an online control panel for a home security system, choosing settings for each member of their household. Although we included options that make monitoring transparent to teens without impacting home security, few parents used these options. Instead, all 19 parents chose either to audit their children without giving them any notice or to receive real-time alerts when their children locked or unlocked the door.

Although all parents in the interview study chose the photo log, which has security benefits yet could place teens under parental surveillance, we found these parents' attitudes about monitoring teens to be nuanced. Some would rather not monitor teens to increase trust. Our follow-up study, however, shows that simple privacy options to make monitoring transparent to teens may not be effective. Even though these options do not impact home security, few participants chose to use them. We conclude with a discussion of other potential interface modifications that retain the benefits of home-entryway security systems while letting parents decide the extent to which they monitor, or do not monitor, teens.

## RELATED WORK

While technology in the home can bring many benefits, it can also have unintended consequences. For example, Brush et al. interviewed inhabitants of smart homes, finding instances of family members sitting in the dark due to a system's unpredictable behavior and intimidating user interface [5]. We build upon work investigating how household devices with sensing capabilities can raise privacy concerns. For instance, Choe et al. deployed "sensor proxies" in 11 households, finding tensions among household members around the adoption and use of in-home sensing applications [6]. Oulasvirta et al. instrumented ten households with sensors for six months, finding that ubiquitous sensing caused anxiety and led to changes in behavior [20]. Finally, Brush et al. documented 11 households' security and privacy concerns related to sharing camera data in a digital neighborhood watch [4].

Changes in technology can particularly impact teenagers, whose communication is often mediated by technology [16, 17]. Marwick et al.'s review of the teen privacy literature identified a paucity of studies investigating technology's interplay with parent-teen relationships [17]. Similarly, Rode asserted that "children's privacy is not taken into account in computer architectures" [22]. Edwards and Grinter noted the importance of examining social implications of household technologies, such as how technology changes norms around "good parenting" [10]. More recently, boyd summarized a decade of fieldwork investigating privacy from teens' perspectives [9]. She described the process through which teens achieve privacy as a negotiation with parents, often starting from a default of "no privacy." Czeskis et al. proposed using value sensitive design to mitigate parent-teen tensions around monitoring [8]. We instead focus on a scenario where monitoring teens may or may not be a goal of adopting the system.

The psychology literature is filled with work analyzing teen-parent relationships. Researchers have delineated parenting styles, such as "authoritarian" and "indulgent" [13]. Petronio described "parental invasive behaviors" and outlined "children's defensive behaviors" in response [21]. She noted parents' and teens' divergent expectations of independence may cause conflict. In a longitudinal study, Hawk et al. found teenagers' perceptions of parental privacy invasion cause conflict, yet the magnitude of conflict differs by family [11].

As Yardi and Bruckman documented [27], parents differ in the extent to which they choose to monitor and restrict teens. Metzger et al. studied 508 parent-teen dyads, finding that

parent-teen trust and privacy attitudes inform monitoring decisions [18]. Parents must strike a delicate balance when making decisions about monitoring; Marwick et al. note that many teenagers believe surreptitious monitoring violates their privacy [17]. Otherwise, as Livingstone and Bober assert, strict monitoring can "undermine the democratic negotiation of mutual rights, trust and responsibilities between parents and children" [14]. Rode identified strategies parents use to enforce rules about technology [22]; while some parents use software tools to monitor teens, others prefer to rely on dialogue. Madden et al. found that half of parents have used parental controls or other digital parenting mechanisms [15].

The door-lock auditing interfaces we used in our study would enable parents to track their teens' comings and goings. Researchers have investigated parental location tracking more broadly. In a survey of 920 parents, Vasalou et al. investigated why few parents adopt technologies for tracking teenagers' locations [26]. Despite added peace of mind, parents felt such systems could negatively impact their children's independence and parental trust. Boesen et al. similarly investigated location-based services, highlighting how teens' perceptions of parental surveillance can harm family trust [3]. In contrast to parental location-tracking technologies, the home security system we investigate provides security and convenience benefits for all members of a family, in addition to the capability of surveillance for teens. Because of the conflation of home security and teen surveillance, the system we investigate raises distinct concerns and consequences.

## INTERVIEW STUDY: METHODOLOGY

We conducted semi-structured interviews with 13 teenagers and 11 parents of teenagers, all from different households.

### Recruitment

We recruited participants in July and August 2013 from a pool of thousands of individuals who had registered with Microsoft's usability recruiting service in the Seattle metro area. We only recruited teenage participants who were about to enter grades 9–12. We excluded prospective participants who did not have a computer or a Facebook account as they might not be sufficiently engaged with technology to form opinions about domestic technology. We required adult participants to be the parent or guardian of a teenager who would qualify for the study and who lived with them over 50% of the time.

Participants chose either a \$50 Amazon.com gift card or Microsoft product of similar value as compensation. We compensated participants generously because all individuals under 18 needed to bring a parent/guardian to give consent.

Due to our ethical obligation to obtain parental consent, we may have excluded teenagers whose parents were unwilling or unable to accompany them to the study, disproportionately excluding children of single parents or those with strained family relationships. The recruiting service, which primarily recruits for usability studies, may be similarly biased towards more affluent families. We accepted these biases as this was a formative study designed to elicit rich qualitative data from participants, not to quantify the incidence of behaviors. That

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

Figure 1. The photo log, one of three auditing interfaces we investigated.

said, we expect that privacy concerns identified by participants with a parent supportive of a teen’s participation in our study would be no less prevalent in the general population.

#### Protecting participants

Our interview covered topics that might cause teens harm or embarrassment if their answers were revealed to their parents. To protect participants, we minimized the information given about the study during recruitment and only recruited one participant per household. Teens could control what parents learned about the exact questions asked, enabling us to discuss topics that would have posed greater risk had we used parent/teen dyads. We obtained consent to participate in the study using Microsoft’s standard participant agreement form without study-specific information. Parents who accompanied teen participants waited far from the interview room.

In reporting our results, we sometimes reveal less about participants than is common in similar studies. In a few cases, we do not attribute quotes to a particular participant.

#### Interview structure

We conducted all interviews in conference rooms. Our scripts for parents and teens mirrored each other as closely as possible. The primary difference between the parent and teen scripts was that we asked teens additional questions about practices common among their friends, whereas we asked parents about motivations for monitoring their teens. To avoid biasing participants to focus on privacy, we initially presented the interview as an investigation of smart homes, with Internet-connected door locks and entryway cameras as example technologies. We never used the word “privacy” unless a participant brought it up. We designed the interview based on a review of prior literature on parent-teen relationships and refined the interview with seven pilot participants.

We first asked participants for consent to record the interview, noting that they could later ask us to discard all or part of the recording. We then administered a parenting-style survey [13] used in the psychology literature. For parents, we rephrased this survey, which was originally written for teens.

*Household composition and technology adoption.* We first explored their familiarity with domestic “smart” devices, including Internet-connected security cameras and lights.

*Commercially-available door locks.* Next, participants reviewed advertising materials from lock manufacturers describing the features of Internet-connected door locks. We solicited participants’ opinions of these locks. We also asked whether they had concerns about having such locks in their home. We then asked participants about their use of traditional keys and history of being locked out or burglarized.

*Auditing home access.* Participants then reviewed printed mock-ups of three interfaces for auditing an entryway door lock. The first interface, *text log*, listed when the door had been locked or unlocked, as well as whose smartphone or PIN was used. The second interface, *photo log* (Figure 1), added photos showing who came in or out. To suggest that visitors’ images would also be captured, one photograph showed two people walking through the door together. We represented the third option, having *no log*, with a blank piece of paper. This option was the most private, yet the least useful for security. We asked participants which interface they would prefer if their house had Internet-connected door locks, and why.

*Existing parental monitoring.* Finally, we asked questions about how parents currently restricted or monitored teens, including both technical and non-technical means. We also asked teens to what extent they or their friends had circumvented rules or monitoring. We concluded by asking whether the participant was comfortable with their household’s current practices of monitoring and restricting teenagers.

#### Analysis

Two researchers who had moderated the study and who had both been in the room for all interviews independently read through transcripts of all interviews and tagged quotes deemed explanatory or otherwise interesting. We collected all 1,852 quotes that one or both of these researchers had tagged.

The two researchers then collaboratively analyzed these quotes using affinity diagramming [2] based on a grounded theory approach. The authors iterated on and refined themes that emerged from this bottom-up affinity analysis. In the end, we identified 28 themes centered on the benefits participants perceived in installing Internet-connected locks and cameras, conflicts that would arise from the adoption of the locks, strategies for minimizing conflict, and parent-teen trust.

#### INTERVIEW STUDY: PARTICIPANTS

Thirteen teenagers (six female) and eleven parents (seven female) took part in our interviews. We list their demographics in Table 1. Teen participants ranged in age from 15 to 17, while parent participants ranged in age from 35 to 59. Three of the teens were entering 10th grade, eight were entering 11th grade, and two were entering 12th grade.

While most participants lived in dual-parent households, T2 lived with a cousin who served as her guardian, and both P4 and P10 were single parents. T8 lived with a step-parent, while P1 and P11 lived with partners who were not their

teens' parents. P11 and T8 lived in three-generational households. T8 and T10 had no siblings, while the other teen participants had one or two siblings. P4 and P10 each had one child, while the other adults had two or three children at home.

Our participants were technologically savvy. All households had a video game console and, due to our screening criteria, at least one computer with Internet access. All adults and all but one teen had a mobile phone. Although only one participant (P4) currently uses an Internet-connected door lock, others had visited a house with such locks (P3, P7, T1, T10), seen commercials on TV (P1, P3, P10, T11), or used home alarm systems or smart thermostats (P1, P4, P8, T9, T12, T13).

All participants lived within a 90-minute drive of Microsoft's campus in Redmond, WA. Eight teens had received their driver's license and four had their own cars. While most participants reported living in an urban or suburban area, P3, P6, T9, and T11 all reported that they lived rurally. Though no participants mentioned living in an unsafe area, five teen participants reported having been victims of household burglaries in the prior two years, one parent participant reported that their neighborhood had recently been burglarized repeatedly, one parent participant reported that their home had been burglarized in the past year, and two other parent participants reported that their homes had burglarized in the past.

Three participants reported work or family circumstances relevant to keys and monitoring. P3 explained that she ran her own pet-sitting business and held copies of keys for numerous homes. She noted that a number of her customers have Internet-connected door locks. P5 reported owning 14 apartments, which he re-keyed himself using a locksmithing kit. P11 reported that one of her daughters had previously struggled with drug addiction, leading to 24/7 monitoring.

We present participant demographics and the results of the parenting-style questionnaire [13] in Table 1. We calculated scores for parental *involvement* and *strictness* on a scale of 0 to 1, where 1 indicates the most involved or most strict. All parents scored themselves highly on involvement, whereas teens' impressions of parental involvement varied. Both groups gave varied responses along the strictness dimension.

## INTERVIEW STUDY: RESULTS

We present our results in four parts. First, we discuss benefits participants perceived in adopting Internet-connected door locks. Second, we present parents' and teens' clashing preferences for what data should be included in audit logs. Third, we unpack this result by examining decisions about audit logs relative to current monitoring strategies, families' parenting styles, and households' histories of burglaries. Finally, we explore unintended consequences of home-security systems: reduced parent-teen trust and reduced home security.

### Internet-connected locks have broad appeal

The majority of both parent and teen participants reported seeing substantial benefits in adopting Internet-connected locks. Cost was the primary drawback, suggesting that more homes may adopt the technology as prices drop. Most participants reported these locks to be convenient (e.g., "because

ID	Sex	Age	I	S	ID	Sex	Age	I	S
T1	F	16	.87	.71	P1	M	35	.85	.83
T2	F	15	.72	.82	P2	M	52	<b>.97</b>	.75
T3	F	16	.73	.82	P3	F	51	.88	.91
T4	M	16	.68	.75	P4	F	46	.92	<b>.97</b>
T5	M	17	.93	.79	P5	M	51	.88	.91
T6	M	16	<b>.97</b>	<b>.83</b>	P6	M	59	.93	.76
T7	M	17	.78	.61	P7	F	46	.93	.93
T8	F	16	.85	.69	P8	F	44	<b>.97</b>	.67
T9	M	15	.70	.56	P9	F	42	<b>.83</b>	.52
T10	F	15	<b>.97</b>	.67	P10	F	42	<b>.83</b>	<b>.45</b>
T11	M	17	.85	.63	P11	F	57	<b>.97</b>	.89
T12	F	16	<b>.50</b>	<b>.38</b>					
T13	M	17	.60	.76					

**Table 1. Interview participants: Teens are identified by T\* and parents by P\*. We indicate each teen participant's perception of their parents', and parents' perception of their own, involvement (I) and strictness (S) from the parenting-style questionnaire [13]. Higher numbers indicate more involved or more strict. We bolded the highest and lowest scores.**

you can lock doors from somewhere else." {T2}), to enhance control (e.g., "because it just gives you more control and also it tells you about people's comings and goings" {P11}), and to improve safety (e.g., "I would feel like, more like safe I guess, because you can tell if your door is locked" {T9}).

Only two parents and one teen did not see connected locks as desirable. P5 had considered installing such locks, yet had not found a compelling reason to do so, saying "I have basically the same schedule as my kids, so they're not home when no parents are home." Living rurally, P6 saw few benefits in connected locks. T10 did not like the idea because "it's cooler to be able to carry your personalized key."

### Parents want photo logs, whereas most teens don't

After showing mock-ups of the three log options (photo, text, none), we asked, "If your family were to install Internet-connected door locks in your home, which interface would you personally prefer your house had, and why?" We allowed participants to examine and ask questions about each option.

*All eleven parent participants chose the photo log.* The predominant justification was safety (e.g., "For safety purposes, you could see who actually was in most of the time" {P7}). Among safety reasons, participants commonly wished to use the camera for identifying robbers ("You need to catch a burglar on camera." {P4}; "I think the biggest advantages...[are] if there was a break-in or a theft." {P10}).

Of the eleven parents, only three (P4, P10, and P11) said they chose the photo log for the purpose of monitoring their children. These three parents were concerned about their children bringing home friends or romantic partners (e.g., "As my son gets older, I'm going to need to verify if he's coming home alone" {P4}). Interestingly, three other parents said they expected their teenagers to dislike the photo log. P2 explained, "It's just a human nature thing that nobody likes when people keep tabs on anybody," while P6 worried, "I think [my children] would be paranoid or intimidated by the photos." Similarly, P9 mentioned, "I don't think my daughters would like me knowing when they lock and unlock the door." Nonetheless, these three parents still chose the photo log.

Some parent participants who chose the photo log said they did not plan to use it often. For example, P1 called the photos “just an extra added feature that’s nice to have,” while P9 mentioned, “I don’t think I would access it.” Most commonly, participants wanted the photo log in case of a problem: “The only reason I would look at this is if there was a problem. If like something happened, something got stolen or something...I won’t be viewing it just to spy on people.” {P3}.

*Six of the thirteen teenage participants chose the photo log.* The rest chose either the text log (T1, T10, T11) or no log (T7, T8, T12, T13). Similar to parents, teens thought photos made it easy to see “if anyone is trying to get into my house” {T4}. Surprisingly, two of these six teens said it would always be okay for their parents to audit their comings and goings.

However, the other four teenage participants who chose the photo log expressed concerns about auditing. T6 had a “very open relationship” with his parents, yet did not want his parents to access the logs all the time. He explained, “If I’m having someone over, then it would just be kind of weird that they could just always look and see exactly who’s over.” T9 wanted his sister not to access photo logs, reporting, “She can often be a little bit judgmental of my friends.”

The three teens who chose the text log said security was important, yet felt the camera would not add much. T1 said the camera was not “quite necessary,” while T10 wanted the camera to take pictures only if people at the door were not “recognizable.” Similarly, T11 was uneasy with surveillance. He said, “With the photos, I don’t know because that seems like an invasion of privacy, well, ‘big brother’ kind of thing.”

The remaining four teens preferred no log. They were most concerned about the adverse effect on teens’ social lives. T8 pushed back against the notion that only misbehaving teens would be concerned. She said, “[The photo log] would pretty much ruin like a strict parent’s kid’s social life. But, the strict parents of my friends, they’re really good kids.” Teens’ preferences against the audit logs were strong (e.g., “It really infringes on your freedom” {T7}; “I would not like that at all...This is like parents going psycho.” {T8}).

In the end, parents felt security concerns outweighed teen privacy, whereas many teens felt otherwise. T13 summarized the tension between using logs for security and for surveillance, explaining, “[The photo log] would be kind of good and bad. Like that parents can know who has gone in the house and it wasn’t us and who it was, but bad for the kids who want to be independent and then the parents know what you’re doing.”

### **Unpacking auditing decisions through current practices**

Parents viewing teens’ comings and goings in an audit log is tantamount to monitoring. To understand participants’ choice of audit log, we investigated each household’s current practices of monitoring teens. While parents are ultimately responsible for their children and have the legal right in most circumstances to monitor their children, our parent participants reported an array of monitoring attitudes and practices.

On an abstract level, all parents considered it ethical to monitor teens (e.g., “You have to monitor what you’re responsible

for.” {P11}). Surprisingly, eight teen participants concurred that this practice is ethical. The remaining five teens said the ethics depended on the circumstances; none claimed it was wholly unethical. These teens commonly cited text messages as off limits. They noted downsides, saying that monitoring leads to circumvention (e.g., “If you do it too much, [it] can cause [teens] to sneak out.” {T12}) and delays social development (e.g., “[My parents] used to [monitor] when I was younger, so I used to be really sheltered.” {T8}).

Few participants reported that parents in their household monitored teens’ computer use. Four parents and one teen reported parents going through teens’ browsing history in the past. Two parents and two teens reported that their household had used parental control software at some point, though both teens’ parents had stopped using it out of annoyance with overly strict blocking. P4, the most strict parent, still used parental control software, but only for a special-needs child. Practices around passwords were polarized. Six parents and six teens reported that parents knew some or all of their children’s passwords (e.g., “A condition for allowing them to get [an account] is to write [the password] down and to agree not to change it.” {P5}). The remaining five parents and seven teens reported that parents did not know any of the children’s passwords.

Echoing prior work [7], teens said text messages were their most private communications. As a result, teens had strong opinions about parents monitoring their phones (e.g., “If they really do check my text messages and check my calls, I don’t really feel comfortable...That’s my own personal information.” {T5}). Eight parents and seven teens reported that parents in their households do not monitor teens’ text messages, often out of respect (e.g., “I don’t think that’s right to touch their phones” {P3}). In contrast, three teens and three parents reported that parents do monitor texts and calls. The remaining three teens reported that their parents have the ability to monitor their phones, yet have chosen not to.

Both parents and teens distinguished between the right to monitor teens and actual monitoring. As T3 said, “[My parents] have free reign of my phone if they want to look at it. But normally, they don’t look at it.” They also distinguished between different children. P11 said she monitored everything one daughter did due to prior drug addiction, yet she never looked through her other children’s phones because “they would consider that a privacy violation.”

### *Monitoring practices versus auditing decision*

We next categorize parent participants’ approaches to monitoring their teens. Two parents monitored their children at all times. Three other parents chose never to do so except in an emergency, even though they said monitoring was ethical. The remaining six parents chose to monitor selectively.

*Style 1: Unconstrained monitoring.* Two parents currently or previously engaged in unconstrained monitoring. P4 monitored her son closely, describing her parenting motto as ‘trust but verify.’ She stated, “If [my son] doesn’t like the rules, then he can go live somewhere else.” The logs she collected included browsing activity on the computer and all technology-

mediated communications (e.g., “I have all the passwords to all of his devices...[I see] what he’s chatting about on Facebook, those sort of things.” {P4}). She noted the great responsibility she felt as a single parent to keep tabs on her son.

When his children were younger, P2 had also engaged in relatively unconstrained monitoring, feeling it was his responsibility to do so. He explained, “I think you do have to keep track of your kids. I think it’s really important...It is really easy for kids to get into trouble these days.” Although he noted, “We [previously] looked at the history on the websites and all that kind of stuff,” he and his wife had ceased doing so when his children were in high school. He noted the delicate tradeoffs in making monitoring decisions by saying, “We want to make sure that they’re safe...We know that they’re going to experiment and do certain things, but we also don’t want to smother them.” While he noted that the photo log would have been essential when his children were younger, he said he did not feel strongly when choosing the photo log.

Full access to auditing logs of a teen’s activity without any additional privacy provisions would support this parenting style. P4 was particularly excited about using the lock system we described. In fact, P4 had already installed Internet-connected door locks, albeit without a security camera. Without her son’s knowledge, she receives automated notifications from the lock when he gets home. She expects him to send a text message anyway and is waiting to receive a text message from him without the lock’s accompanying notification.

*Style 2: No monitoring.* Three parents (P1, P7, P10) used the opposite parenting style and chose not to monitor their teens. Most commonly, they cited trust as the reason for not monitoring their children (e.g., “I trust my kids...The more responsible a person’s going to be, the more freedom you’re going to give him.” {P7}). P10 expanded upon this idea, saying, “I just tended to trust him more...It was letting him use his own judgment...I think it’s a relationship more about respect, and I’ll give him trust automatically.” These participants also mentioned that their children had not given them reason to be concerned (e.g., “I’m just waiting to see if she gives me a reason not to let her just, you know, be free.” {P1})

None of these parents knew any of the children’s passwords, nor did they ever look through their children’s messages. They did not want to do so. For instance, P7 mentioned that she was aware of other parents taking teenagers’ phones away at night or looking through their text messages, yet objected to using either practice with her own children. P10 described the computer being located in a living room up until a year ago as sufficient, explaining “That was my monitoring.” In the last year, she has also permitted her son to take the computer into his own room without any monitoring.

Although all three deemed it ethical to monitor teenagers, they had currently chosen not to do so for their own teenagers. They felt this decision would promote trust in the parent-teen relationship. However, all three of these parents chose the photo log. Both P1 and P7 said this decision was made entirely for security purposes (“You may have thought it was them, but then you find something missing or whatever.”

{P1}; “Just for safety purposes.” {P7}). P10, however, was influenced by particular circumstance in which her son held a party when she was out of town. She did not want to monitor her son regularly, but wanted to prevent these sorts of parties.

*Style 3: Intentionally limited monitoring.* The remaining six parents had stockpiled the tools with which to monitor their children. However, they chose to monitor their children only in particular and limited circumstances. A common example of this style was a parent who knew their children’s passwords, yet felt it would be wrong to use the password without good reason. For example, P5 explained, “Even though a precondition for doing Facebook was that they give me their login, I feel like that’s a violation of their privacy if I were to [log on]. I know that I have their permission, I know that I have the access, but that’s going further than I want to.”

These parents said it was natural not to know everything, yet did choose monitor to an extent. For instance, P8 said she previously kept track of her children’s passwords, yet had recently stopped, conceding, “The less we know, probably the better it is.” P9 specified that she had instructed her children “never to share their password with anyone,” including her. However, if she demanded to see their phone if they were “in big trouble,” she expected them to hand it over unlocked.

Parents adopting this parenting style may or may not want to monitor their children’s comings and goings. Therefore, they are left with a complex choice. On the one hand, they can choose to monitor the audit logs closely for the purpose of security, yet they are also monitoring their children as a consequence. On the other hand, if they do not want to monitor their children other than in specific circumstances, they cannot monitor for security purposes.

When we asked why they chose the photo log, four of these six parents did not mention monitoring their children among their reasons. Some parents even suggested they might not want to monitor their children in most circumstances (e.g., “I wouldn’t necessarily want to be notified just if one of my kids walked through the door.” {P5}). While surveilling their teens may have been a secondary goal, it did not appear to be their primary goal. They instead mentioned the security benefits of these logs (e.g., “I would prefer [the photo log] especially if I was allowing people I don’t know to come in and out.” {P9}) Notably, P11, one of the two parents who did mention monitoring children among her reasons, explicitly said that monitoring her children was secondary to documenting intruders who got hold of someone’s access code.

#### *Parenting style versus auditing decision*

While intuition might suggest that teenagers with strict parents would be opposed to the photo logs because these strict parents would have more information about the teens, we found precisely the opposite. Five of the six teens who rated their parents as comparatively most strict on the parenting-style survey preferred the photo log. In comparison, only one of the remaining seven teens, who rated their parents as comparatively less strict on the survey, chose the photo log.

One possible explanation of this counterintuitive result is that the extra information on teens’ comings and goings provided

by the photo logs would not change the relationship or power dynamic between strict parents and their teenagers. This phenomenon can be understood by examining prior work by Troshynski et al. [24] and Shklovski et al. [23]. Troshynski et al. proposed the term “accountabilities of presence” as an alternative to “location privacy” in describing how information about an individual’s location is crucially understood as their presence or absence at a socially constructed location holding them accountable to different social relations. Shklovski et al. extended this work by examining how the more precise information about a parolee’s location presented to his or her parole officer through GPS bracelets impacts the power dynamic and relationship between the parolee and parole officer. In our case, the less strict parents currently have comparatively less information about their teens’ comings and goings. The photo log’s extra information would therefore substantially impact the parent-teen power dynamic.

A possibly complementary explanation is that the photo log would enable teenagers with strict parents to document their compliance with parents’ exacting requirements. In an example of similar behavior, one of P8’s daughters would constantly remind her to check her exemplary grades online.

Because all parents chose the photo log and all parents rated themselves highly on involvement, we only compared parents’ self-assigned strictness scores on the parenting-style survey to the aforementioned monitoring style we felt best described each parent’s philosophy toward monitoring their children. P4, who engaged in unconstrained monitoring, unsurprisingly rated herself higher on the strictness dimension than any other parent participants. In contrast, P2, who previously engaged in unconstrained monitoring, gave himself the eighth highest strictness score of the eleven parents. The strictness scores for the three parents who chose not to monitor their children, however, ranged from second most strict (P7) to least strict (P10). In essence, strictness scores had a fairly weak relationship to monitoring philosophies.

#### *Burglary history versus auditing decision*

Five of our teen participants had their home burglarized in the past two years. Three of our parent participants had also been victims of a home burglary, though all but one of these burglaries had occurred many years prior. Another parent participant lived in a neighborhood that had recently experienced a spate of burglaries, leading the neighborhood residents to come together and purchase surveillance equipment.

While we expected the five teens whose houses had been burglarized would choose the photo log for its security benefits, we did not find a strong correlation between burglaries and which audit log the participant chose. Two of these five teens chose the photo log, one chose the text log, and two preferred no log, roughly mirroring the overall distribution. Despite one teen’s mother having lots of jewelry stolen and another teen having her bicycle stolen in home burglaries, these experiences did not appear to drive these teens’ decisions.

Of the four parents who had experiences with burglaries, only one explicitly mentioned the ability to photograph a burglar as an advantage of the photo log. This participant had already

pretended to have video surveillance when she suspected that a relative was stealing things from her home. She explained, “I had lied and said [to my relative], ‘You know, I have a video of you at our house’...I sure wish I would have had a video.” Two of the other parents, however, alluded to the “extra information” contained in the photo log without explicitly mentioning the ability to document burglars.

#### **Consequences of deployment**

We observed two unintended consequences of the audit interfaces. Parent-teen trust was threatened by teens’ perceptions of surveillance. Furthermore, teens’ circumvention of the system would leave a home vulnerable to intruders.

*Reduced teen-parent trust.* Although all of our participants appeared to have positive parent-teen relationships, we observed cases in which parent-teen trust would be negatively impacted by auditable smart-home devices. For instance, two teens volunteered that they would spend their time at the house of a friend with more relaxed parents if their own parents were to install auditable locks and cameras.

By the same token, some parents said they loosened the reins on their children to engender trust in their parent-teen relationship. For instance, P8 chose to give her children space, saying, “If you’re too strict, they go do things to circumvent it.” Other parents similarly chose not to take monitoring steps that they could (e.g., “We try to give the kids the benefit of the doubt” {P2} and “The more responsible a person’s going to be, the more freedom you’re going to give” {P7}).

*Circumvention reduces security.* Echoing prior studies [9,27], our teen participants shared with us a repertoire of practices that they currently employ to circumvent monitoring imposed by their parents. Some of these approaches already reduce home security. For example, one teen described disabling an existing window contact sensor, explaining that “if you put on another metal thing, it doesn’t actually detect anything.”

Teen participants also shared numerous ways they would circumvent the lock-and-camera system. Some of these actions would reduce the security of the home. Four teens said they would unplug, disable, or cover a home security camera to avoid conflict with parents. Five teens said they currently sneak out, and many teens said a security system would not deter them; they would leave the door or a window unlocked the entire time they were out of the house. One teen already climbs out the window at night after the parents are asleep. Teen participants reported such practices would become far more prevalent if their door locks were auditable. One participant said, “I would have to yell like, ‘Oh, Rapunzel’...and have to climb the wall” when we asked what would happen if security systems were installed at a significant other’s house.

#### **ONLINE CONFIGURATION STUDY: METHODOLOGY**

Although all parent participants chose the photo logs in the interview study, some reported that they would try to provide privacy and autonomy to their teens. In order to see whether parents would apply this ideal in practice, we performed a second study in which we asked parents to configure Internet-connected locks and cameras they believed might be

deployed in their own home, with configuration options that offered teens increased privacy. In particular, we explored two options: one that keeps a teen’s logs private by default, requiring parents to obtain the permission from the teen to view the logs of her comings and goings, and one that notifies the teen when her logs are viewed.

The most ecologically valid approach to studying parents’ choices would be a field study in which participants deployed an auditable lock system in their homes. Lacking a ready-to-deploy system, we instead had participants configure an online control panel for such a system under the pretense that the configured system might be delivered for a field study.

### Recruitment

To target our experiment to households with teens, we initially recruited for a participant pool interested in “research studies on smart homes.” We invited only households with teenagers from this pool to participate in this study. We recruited for our participant pool by posting classified ads on Craigslist<sup>1</sup> and Backpage.<sup>2</sup> We recruited nationally on Backpage. To comply with the Craigslist terms of service, we advertised sequentially in Pittsburgh, where CMU is based, as well as four metropolitan areas in which Microsoft has offices: Boston, New York City, San Francisco, and Seattle.

We asked prospective participants to indicate their interest in participating in online and in-situ studies of smart homes. We asked for each household member’s age, gender, and relationship to the prospect (e.g., parent, daughter). We required participants sign a consent form that covered future online surveys and configuration experiments related to smart homes. In total, 514 prospects registered for the participant pool.

We emailed the 73 prospects who had children eleven years of age or older at home and who were willing to do both in-situ and online studies. We invited them to “participate in a study of electronic locks and lock-triggered cameras for the exterior door(s) of homes.” We explained they would “configure an electronic lock system that allows you to lock or unlock the entryway door to your home using a PIN code or smartphone application.” We offered a \$15 gift card as compensation.

### Instructions

To encourage participants to configure the system as they would deploy it in their own home, we explained that “some participants may be selected to join a field study in which they would receive electronic locks for the exterior doors of their home.” Participants needed to verify that they would be willing to deploy the system in their own home and that they would not disclose information about the prototype system.

We then informed participants that they would configure a lock-management system for their home. We wrote that the system “pairs locks with cameras placed at entryway doors.” To encourage realistic configuration, we wrote that participants selected for a field study may not have another opportunity to configure the system until after it is installed.

<sup>1</sup><http://www.craigslist.com>

<sup>2</sup><http://www.backpage.com>



Figure 2. The lock control panel.

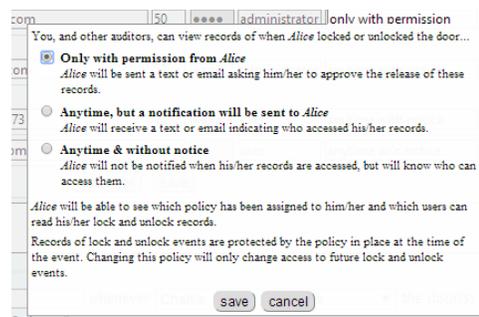


Figure 3. Options for configuring each user’s auditing privacy.

### Control panel

Participants then configured the system using the control panel shown in Figure 2. We prepopulated demographic information provided when registering for the participant pool.

To see whether parents would choose to audit other members of their household, we asked participants to assign everyone a role and audit policy. Roles were *user* (can lock and unlock), *auditor* (a user who can also audit log records), and *administrator* (an auditor who can change settings). We provided three options for audit policies (Figure 3), noting that users would be told which policy had been assigned to them. The least private setting allowed a user’s comings and goings to be monitored anytime without notice. The middle option allowed auditing anytime, but the user would be notified about the audit. The most private setting allowed log records to be viewed only with explicit permission from the user obtained via email or SMS. Participants could also sign up to receive real-time notifications about a user (bottom of Figure 2).

### Post-task survey

Our post-task survey probed why participants chose their configuration. They rated the desirability of different use cases for the lock, including convenience and the ability “to monitor my children’s comings and goings.” To understand the decision-making process, we asked if participants consulted with anyone else while configuring the system. For each user, we asked the participant to explain why they had chosen that auditing policy. Some participants saw this question as an invitation to provide an overall explanation of the settings for that user, which made interpretation of the privacy-versus-

#	Participant		Partner		Age	Child	
	Sex	Policy	Role	Policy		Alerts	Policy
1	F	no notice	admin	no notice	15	yes	no notice
2	F	perm req			19	yes	perm req
3	F	perm req	admin	perm req	13	yes	no notice
4	F	notice	audit	notice	18	not	no notice
5	F	no notice	admin	no notice	22	not	no notice
6	M	no notice	audit	no notice	14	not	no notice
7	F	perm req			14	yes	perm req
8	F	notice	audit	notice	19	yes	notice
9	F	perm req	audit	perm req	16	not	no notice
10	F	perm req			18	yes	perm req
11	M	notice	admin	notice	14	yes	notice
12	F	notice	audit	no notice	14	not	no notice
13	M	perm req	admin	no notice	11	yes	no notice
14	F	perm req			16	not	no notice
15	F	perm req	admin	no notice	20	yes	no notice
16	M	notice	audit	notice	15	not	no notice
17	F	notice	admin	no notice	13	yes	no notice
18	F	no notice	admin	no notice	22	yes	no notice
19	F	perm req			20	yes	no notice

**Table 2.** In the *configuration* experiment, participants assigned settings for each member of their household. We show the participant’s age, sex, and the auditing policy they set for themselves. We also show the role and auditing policy assigned to their partner. For the child given the most private settings, we show the age, whether the parent set up real-time notifications of entries/exits, and the auditing policy assigned. We abbreviate auditing policies as *no notice* (‘anytime without notice’), *notice* (‘anytime with notice’), and *perm req* (‘only with permission’).

security tradeoff difficult. We followed up with these participants by email for clarification and updated the data.

## ONLINE CONFIGURATION STUDY: RESULTS

While most parents configured the online control panel to protect their own privacy, all either chose the ability to audit their teens’ log records without notifying them or configured real-time notifications of their teens’ entries and exits.

Of the 73 individuals invited, 23 participated in the study. One no longer had children living at home, and three participants gave their own email address for all users, preventing those individuals from having control over their privacy or receiving notifications. We excluded these four participants.

We summarize key configuration settings for the remaining 19 participants in Table 2. Five participants were single parents, while 14 had partners. Eight of the 14 participants with partners made their partners administrators, and the other six assigned their partners to the ‘audit’ role. Whereas no participant assigned a partner to the ‘user’ role, all 19 assigned children to the ‘user’ role. In most families with multiple children at home, the parent chose identical settings for all children. In the rare cases where parents assigned different settings, we report only the most private setting.

Most participants chose privacy protection for themselves. Seven (37%) chose ‘only with permission’ as the auditing policy for their account, though the choice was moot for three participants without spouses as they alone had auditing permissions. Two additional participants (11%) chose a policy that would allow others to view their comings and goings, but they did not give any other user audit permissions. Therefore, we also categorize these participants with their effective policy of allowing others to audit them ‘only with permission,’

meaning a total of nine participants explicitly or implicitly had this policy for themselves. Six participants (32%) would allow their partner to audit them with notice, while only four (21%) would allow them to audit without notice.

The 14 participants with partners were somewhat less generous with their partners’ privacy. Two participants (14% of those with partners) assigned their partners the ‘only with permission’ policy and four (29%) the ‘anytime with notice’ policy. The remaining eight participants reserved the right to audit their partner ‘anytime without notice.’

Participants chose even less privacy-protective settings for their children. Fourteen participants (74%) configured accounts such that the teens could be audited at any time and without any notice given to them. All five remaining participants set up real-time notification of their children’s comings and goings. As a result, all 19 teens would be monitored without notification or consent. We did not specify whether real-time notifications contained photos, so parents may have thought this configuration somewhat protected teens’ privacy.

In open-ended responses at the end of the study, parents provided a range of explanations for configuring the lock manager in a way that would enable them to surveil their teenagers. One participant said she chose to be able to audit her daughter ‘anytime without notice’ because “she doesn’t have anything to hide, so it shouldn’t be a problem.” Another participant simply stated, “I’m the only one who needs to know.” One parent who configured the system to notify her daughter when an audit occurred said she chose the option that best preserved existing trust, explaining, “We have close communication so I was fine with that.”

The configuration options we investigated in this study can help parents either avoid monitoring teens’ comings and goings or make this monitoring transparent while still maintaining the security benefits of the system. Even if burglars use a teen’s access code to enter the house, parents can ask the teen to look up access logs (if ‘only with permission’ has been chosen) or the parent can look up the corresponding logs themselves knowing that the teen will be notified (if ‘anytime with notice’ has been chosen). In our study, however, few participants chose these options. Our understanding of their intent is limited to post-task survey responses. Furthermore, a one-time, online study does not capture the parent-teen negotiation that often governs teenagers’ privacy from their parents [9]. In future work, we hope to more fully explore a wider range of configuration options among a larger number of parents with distinct parenting styles.

## DISCUSSION

Technologies like the locks and entryway cameras we investigated can alter privacy dynamics in the home. While creating an audit log of what happens in and around a home can be very useful for maintaining the security of a home against burglars, as well as potentially for debugging the devices in a smart home when they behave unexpectedly, the information these devices record can be considered tantamount to surveillance in certain circumstances. Surveillance in the home can be a particularly fraught topic, with a history of debate on

topics ranging from spousal wiretap [25] to teen privacy [17]. Furthermore, parents' attitudes on monitoring their teens can sometimes be contradictory. As described by Nelson [19], parents sometimes espouse a philosophy of giving teens independence, yet in practice closely monitor their teens.

The system we examined contrasts in important ways with existing home-security systems. Traditional burglar alarms are disabled by entering a secret code, and this activity is generally not logged unless an alarm triggers a call to law enforcement. Even "nannycams," cameras hidden in the home to detect untoward behavior by caretakers toward children, have fundamentally different characteristics than auditable locks and entryway cameras. Parents often hide nannycams in the rooms where children play, rather than in entryways. By virtue of knowing where the nannycams are located or even just by avoiding younger children's play areas, members of the household can likely avoid being caught on camera.

While the obvious approach for giving teens privacy would be to disable systems' auditing features, this approach would unfortunately eliminate the security benefits of auditing. Even though we provided participants in our second study options that make monitoring transparent to teens without affecting home security, few participants used these options. In this section, we speculate on additional interfaces and approaches that could maintain the security benefits of detailed access records while minimizing the impact on teens' privacy. Teens generally obtain the right to privacy in the home through a negotiation process with their parents [9]. We imagine these proposed approaches would enable a negotiation that empowers parents to decide how much privacy their teen's maturity warrants while keeping the home secure in all cases.

#### *Outsource auditing*

Rather than enabling individuals to monitor other members of their family, the family could outsource the auditing to a third party, such as a company specializing in home security. However, privacy and trustworthiness concerns about having strangers, albeit professionals, monitoring the entire family cast doubt on this approach. In fact, only two teens in our interview study said they would always be okay with granting a security company access to this data.

A more promising idea that we leave as future work is to outsource auditing to the individual being monitored. For instance, when Alice's credentials are used to open the door, the system could automatically email or text Alice's phone asking her to verify that she actually entered. If Alice does not respond or if Alice denies that she unlocked the door, the system would raise an alarm. In essence, Alice would serve as her own monitor. However, it is essential that a burglar who steals Alice's phone should not be able both to unlock the door and to "verify" that Alice unlocked the door without additional safeguards (e.g., a PIN code).

#### *Technology-assisted auditing*

Rather than outsourcing auditing responsibilities to people, one could instead use technology to perform some or all of the auditing. As one of our participants suggested, if a system verifies through face-recognition technology that a mem-

ber of the family is entering the house, the system may not need to add that event to the audit log. That said, the system may still want to record that event in a backup log in case an adverse event has occurred. That entry, however, would not be casually accessible through the primary audit logs.

In a similar vein, context-sensitivity could be taken into account when creating audit logs. For instance, the system could determine whether or not to add events to the audit logs based on the time of day or based on who is home, taking into account the preferences of the household's decision makers. Although it would be prudent to retain all data the system collects in case of emergency, the main audit logs could omit entries from when members of the household were home.

#### *Privacy through reduced visibility*

While privacy is commonly achieved through restricting access to content, one can also achieve privacy by making information harder to find [1]. One way to reduce the visibility of logs is to make the log accessible only on a website ("pull" access), rather than through automatic notification ("push" access). If parents suspect either a burglary or a transgression by their teenagers, they could visit a secure website to view audit logs. If everything in the home appears copacetic, the parents would be unlikely to audit the logs.

Another approach to making information less visible without necessarily reducing utility is to present less granular logs. For instance, a teenager who pushes an 11:00 PM curfew would prefer a log that says the teen arrived home "around 11 PM," as opposed to at "11:13:42 PM." Parents would need to decide whether choosing to be in the dark about minor violations is an appropriate way to let a teen push boundaries.

## **CONCLUSION**

New technologies have the potential to alter social relationships. In our interview study, we delved into how auditable door locks and entryway cameras in the home might impact the relationship between parents and teens. This topic is of particular importance in light of the increasing popularity of such technologies [12]. While we found that both parents and teens liked the convenience and security benefits such a system would provide, over half of our teen participants were averse to photographs being included in audit logs. In particular, six of the seven teens with the most lenient parents did not want photo logs, likely because their parents would be able to monitor their comings and goings with ease as a consequence of maintaining home security.

In our followup online study examining whether parents would independently configure such a system to protect teens' privacy, all 19 parents opted either to audit their children without notice or to receive instant alerts upon lock or unlock events. Teens, however, acquire privacy through negotiation with their parents [9]. Unfortunately, if decisions about maintaining the security of the home are entangled with decisions relating to teens' privacy, what might teens hope to negotiate? Together, our results suggest the need for new approaches that enable a family to maintain the security of their home while independently enabling parents to decide whether or not they monitor their children's comings and goings.

## REFERENCES

1. Bauer, L., Cranor, L. F., Komanduri, S., Mazurek, M. L., Reiter, M. K., Sleeper, M., and Ur, B. The post anachronism: The temporal dimension of Facebook privacy. In *Proc. WPES* (2013).
2. Beyer, H., and Holtzblatt, K. *Contextual Design: Defining Customer-Centered Systems*. Morgan Kaufmann, 1998.
3. Boesen, J., Rode, J. A., and Mancini, C. The domestic panopticon: Location tracking in families. In *Proc. UbiComp* (2010).
4. Brush, A. B., Jung, J., Mahajan, R., and Martinez, F. Digital neighborhood watch: Investigating the sharing of camera data amongst neighbors. In *Proc. CSCW* (2013).
5. Brush, A. B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., and Dixon, C. Home automation in the wild: Challenges and opportunities. In *Proc. CHI* (2011).
6. Choe, E. K., Consolvo, S., Jung, J., Harrison, B., Patel, S. N., and Kientz, J. A. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proc. UbiComp* (2012).
7. Cranor, L. F., Durity, A. L., Marsh, A., and Ur, B. Parents' and teens' perspectives on privacy in a technology-filled world. In *Proc. SOUPS* (2014).
8. Czeskis, A., Dermendjieva, I., Yapit, H., Borning, A., Friedman, B., Gill, B., and Kohno, T. Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety. In *Proc. SOUPS* (2010).
9. danah boyd. *It's Complicated: The social lives of networked teens*. Yale University Press, 2014.
10. Edwards, W. K., and Grinter, R. E. At home with ubiquitous computing: Seven challenges. In *Proc. UbiComp* (2001).
11. Hawk, S., Keijsers, L., Hale, W., and Meeus, W. Mind your own business! Longitudinal relations between perceived privacy invasion and adolescent-parent conflict. *Journal of Family Psychology* 23, 4 (2009), 511–520.
12. Kurutz, S. Losing the key. *New York Times*, June 11, 2014.
13. Lamborn, S. D., Mounts, N. S., Steinberg, L., and Dornbusch, S. M. Patterns of competence and adjustment among adolescents from authoritative, authoritarian, indulgent, and neglectful families. *Child Development* 62 (1991), 1049–1065.
14. Livingstone, S., and Bober, M. Regulating the Internet at home: Contrasting the perspectives of children and parents. In *Digital Generations: Children, young people and new media*. 2006, 93–113.
15. Madden, M., Cortesi, S., Gasser, U., Lenhart, A., and Duggan, M. Parents, teens, and online privacy. Pew Internet Report, 2012.
16. March, W., and Fleuriot, C. Girls, technology and privacy: “Is my mother listening?”. In *Proc. CHI* (2006).
17. Marwick, A. E., Diaz, D. M., and Palfrey, J. Youth, privacy, and reputation. Harvard Public Law Working Paper No. 10–29, 2010.
18. Metzger, A., Ice, C., and Cottrell, L. But I trust my teen: Parents' attitudes and response to a parental monitoring intervention. *AIDS Research and Treatment* (2012).
19. Nelson, M. K. *Parenting Out of Control: Anxious Parents in Uncertain Times*. NYU Press, 2012.
20. Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., Vainio, N., and Myllymäki, P. Long-term effects of ubiquitous surveillance in the home. In *Proc. UbiComp* (2012).
21. Petronio, S. Privacy binds in family interactions: The case of parental privacy invasion. In *The Dark Side of Interpersonal Communication*. 1994, 241–258.
22. Rode, J. A. Digital parenting: Designing children's safety. In *Proc. BCS-HCI* (2009).
23. Shklovski, I., Vertesi, J., Troshynski, E., and Dourish, P. The commodification of location: Dynamics of power in location-based systems. In *Proc. UbiComp* (2009).
24. Troshynski, E., Lee, C., and Dourish, P. Accountabilities of presence: Reframing location-based systems. In *Proc. CHI* (2008).
25. Turkington, R. C. Protection for invasions of conversational and communication privacy by electronic surveillance in family, marriage, and domestic disputes under federal and state wiretap and store communications acts and the common law privacy intrusion tort. *Nebraska Law Review* 82, 693.
26. Vasalou, A., Oostveen, A.-M., and Joinson, A. N. A case study of non-adoption: The values of location tracking in the family. In *Proc. CSCW* (2012).
27. Yardi, S., and Bruckman, A. Social and technical challenges in parenting teens' social media use. In *Proc. CHI* (2011).