Digital Parenting: Designing Children's Safety

Jennifer A. Rode
University College London,
Interaction Centre
MPEB 8th Floor, Gower St.
London, WC1E 6BT UK
jen@acm.org

ABSTRACT

In this paper, I describe an ethnographic study of children and parents looking at issues of domestic privacy and security. I will provide an overview of parental rules and strategies for keeping children safe and briefly discuss children's perspective on their online safety and how their parents shared the domestic work and responsibility for protecting them. As part of the discussion, I will present implications for design, and reflect on the problematic state of ethics, privacy, ethics review boards when working with children.

Categories and Subject Descriptors

H.5.2 [Information Systems]: INFORMATION INTERFACES AND PRESENTATION (e.g., HCI) – User Interfaces; K.6.5. [Computing Milieux]: Management of Computing and Information Systems – *Security and Protection*; K.7.4 [Computing Milieux]: The Computing Profession – *Professional Ethics*

General Terms

Design, Security, Human Factors.

Keywords

Ethnography, Children, Ethics, Home, Privacy.

1. INTRODUCTION

Family homes include children by definition. Parents focus energy on keeping their offspring safe and secure, and in the modern world, this includes keeping children safe online. Safety and security for children, in terms of keeping them safe from strangers or not making them the targets of viruses or spyware, are subjects of much debate and publicity, but practical studies of domestic security software have not been contributed to the HCI literature.

Children have a complicated position within the HCI literature. Entire conferences such as Interaction Design and Children are devoted to their study, yet in core conferences, only a few papers mention them each year. Similarly, often highly referenced works on privacy do not focus on them [17] or mention them only briefly [13], though focused studies on aspects of youth culture concentrate on privacy concerns related to mobile phones and Facebook [1, 7, 8, 14]. While there is considerable work on domestic routines in the home [3, 23, 24], and domestic privacy concerns [6, 21], children are

often not discussed in relation to these concerns. This is especially problematic given the attention given to keeping children safe in the news [10, 11]. In this paper I explore security of children in the home through an empirical study. In presenting my findings, I will first review the types of rules parents had for keeping their children safe and their strategies for implementing them. Second, I will briefly discuss the children's perspective on their online safety. Third, I will discuss how parents shared the domestic work and responsibility for protecting their children. As part of the analysis of this work, I will present implications for design and reflect on the problematic state of ethics, privacy, ethics review boards, and working with children.

While HCI literature often distinguishes between security, a technical concern, and privacy, a largely social concern, it became apparent during my interviews that for my participants the boundary between “security” and “privacy” was indistinct [5]. Similarly, throughout this paper I will discuss the concept of keeping children safe. The question is then safe from what. The notion “safe” is a member's category for my participants and represents safety from a number of threats including child predators, adult content, keeping children from inadvertently sharing personal information unwisely, as well as, keeping their computer's safe from spyware, viruses, and other types of malware. Thus, when I refer to the notion of “keeping children safe” in this paper I refer back to my participant's colloquial usage.

2. METHOD

This paper reviews a study with two phases.¹ First, we conducted a set of pilot interviews with members of seven households conducted in Symantec's offices, for a total of 16 individuals, including 8 adults and 8 children. In some households, both parents and all children were interviewed, whereas in other households only some family members were interviewed.

Second, in order to understand the domestic ecology of domestic security, I, in conjunction with colleagues at Symantec, conducted an empirical field study in the homes of households with some sort of security software. The data presented here is a subset of a larger study of twenty households [20] and the data here focuses on the subset of the twelve households with children—this includes 35 individual—14 adults and 19 children. In order to allow the data here to be easily cross-referenced with other related publications from this study I have kept the original household numbering out of twenty, consequently some numbers, HH4 for instance, are skipped as they represent households without children. We interviewed all adults and children over the age of seven if we

© The Author 2009.

Published by the British Computer Society

¹ This work was done as part of my professional obligations to my Symantec and done entirely independently of any university affiliation.

HH	Name	Age	Role	Sex	Profession	Employment Status	Ethnicity/ Additional Languages	Household Income	Highest Completed Education
1	Kristin	45	Mom	F	Designer	Self	White	100k+	Bachelors
	Frank*	48	Dad	M	Engineer	Full Time	White	100k+	Bachelors
	Phoebe	12	Child	F	Student	-	-	-	-
	Darren	9	Child	M	Student	-	-	-	-
	Keith	15	Child	M	Student	-	-	-	-
2	Javed	40	Dad	M	Software Engineer	Full Time	White	100k+	Masters
	Karen	36	Mom	F	EMT Student	Student	White	100k+	Masters
	Mia	17	Child	F	Student	-	-	-	-
3	Christina	49	Mom	F	Office Manager	Self Employed	White	Decline ¹	Masters
	Bob- NI	56	Dad	M	Student	-	-	-	-
	Susan	10	Child	F	Student	-	-	-	-
	Clark	8	Child	M	Student	-	-	-	-
6	Yan	40	Mom	F	Biotech Alliance Mgr	Full Time	Asian/ Chinese	150-249k	PhD
	Julie	12	Child	F	Student	-	-	-	-
	Amy	9	Child	F	Student	-	-	-	-
7	Kathy	41	Mom	F	Product Researcher	Self	White	250k+	Bachelors
	Tom-NI	45	Dad	M	Software Consultant	Self	White/ French	250k+	Masters
	Michael	12	Child	M	Student	-	-	-	-
	David	9	Child	M	Student	-	-	-	-
8	Aileen	43	Mom	F	Masters Student	Student	Pacific Islander	Unknown ²	Bachelors
	Matthew	6	Child	M	Student	-	-	-	-
	Chris	3	Child	M	Student	-	-	-	-
9	David	37	Dad	M	Computer Architect	Full Time	White	150-249k	Masters
	Tammy	10	Child	F	Student	-	-	-	-
	Declan	5	Child	M	Student	-	-	-	-
10	Lori	42	Mom	F	Software Marketing	Full Time	White	100-150k	Bachelors
	Ned	6	Child	M	Student	-	-	-	-
11	Lisa	39	Mom	F	Mental Health Provider	Full Time	White	50-74k	Masters
	Ben	5.5	Child	M	Student	-	-	-	-
12	Eric	57	Dad	M	Broadcast Engineer	Full Time	White	75-99k	Bachelors
	David*	18	Child	M	College Student	-	-	-	-
	Kate	16	Child	F	Student	-	-	-	-
	Mary	12	Child	F	Student	-	-	-	-
14	Barbara+G	47	Mom	F	Writer/ publicist	Self	White	150-249k	Bachelors
	Ken+G	51	Dad	M	General Contractor	Self	White/ Spanish	150-249k	Bachelors
	Allison	11	Child	F	Student	-	-	-	-
	Oscar	7	Child	M	Student	-	-	-	-

Key: *=Interview conducted by colleague, NI= Not interviewed, +G= Interviewed together
Households shown here are subset of the larger study. Households #4,5 had no children.
Steps have been taken to protect participant's identity, not children's real names.

felt they were able to provide informed assent. See figure for demographic details.

There were 12 households with children under 18 including four two-parent households with children, four female headed single-parent households, and three male headed single-parent households, one of which had a new platonic roommate, and one couple with a foster child who had just moved out. Within each of these structural types, I observed patterns in how they met their technology needs.

Most of the households with children were in the greater Silicon Valley (HH1-12) area, though there was one in Orange County (HH14). Conducting research in high tech centers that include Symantec offices enabled me to readily access early adopters of novel or newer domestic technologies. As anthropologist Laura Nader's research [16] suggests, by studying such cultural elites insight is gained into technology practices for all technology users. Additionally, similar to Darrah & et al.'s research [4], selection of Silicon Valley early adopters enabled me to see how boundaries of work and home

are renegotiated in response to new technologies; active negotiation within the spheres of home and work was especially valuable because of the complex relationships of gender and technology use across public and private spaces.

In order to learn about domestic technology, I employed an ethnographic approach. In situ studies allowed me to explore the social, physical, fiscal, and temporal environment in which households were making privacy and security decisions and configuring and programming technologies. While in the home, I engaged in interview and observation. Participants were asked to complete pre- and post-study questionnaires, including a special version with smiley-o-meters for children [18]. I brought dinner which I used as an occasion to get to know participants, afterwards I asked them to give me a tour of the technology artifacts as related to computer safety and security in their home and photographed key objects, a technique similar to Kraut et al. [12]. Data was analyzed and grounded theories emerged [22].

2.1 Informed Consent

Next, I will briefly describe the process of obtaining informed consent (adults) or assent (children) as agreed on by Symantec's internal review of this study for ethical implications. I do so because determining how to obtain informed consent was not straightforward, and raises questions for how similar studies should be conducted. In order to participate, all participants had to be able to understand the study in order to be able to provide the permission, which meant we did not interview very young children though during the fieldwork they were present while we interviewed their families.

In order to ensure informed consent, we talked to the parents first and gave them the big picture that included what we are studying; how the data would be used; how we planned on protecting anonymity; and under what circumstances we will provide the parent information about the child's responses. Finally, we clarified that in order to participate, both the parent and child needed to agree and sign the paperwork.

We then spoke to the child(ren), and overviewed the same topics. When appropriate, we let the parent explain, but we made sure the explanation was complete. Researchers always told children they did not have to answer the questions if they did not want to, and often the children, bored by the interview, ran off to watch TV before it was completed.

Two forms needed to be signed. The parent needed to sign a consent form to interview the child(ren). The child needed to sign an assent form to participate (one per child). Adults also needed to provide written consent for themselves. Children's assent forms were compliant with US guidelines for child assent forms.

The reason we were so concerned with informed consent is that we were asking about household rules to keep children safe and secure. We recognized we may encounter situations where the child knowingly or unknowingly violated their parents' rules putting themselves at risk. We felt a moral obligation in those circumstances to inform the parent of the possible safety risk. However, informed consent dictated that we tell the children we were going to do this. We informed both children and parents of this, and we pointed out to parents that under such circumstances children may not give us accurate answers in order to keep themselves out of trouble.

In reality, as I will discuss later, children did break their parent's rules. In some cases there was awareness in the family of all past breaches. In other instances children confided in us during the course of the interview about breaking a rule, but they might not have understood they were doing so. For instance a teenage girl did not realize an email address in the form of `firstname_lastname@gmail.com` constituted sharing her full name online and thus violated her father's rules. Her sister, who was present at the time, mocked her for not thinking this through, but it was quite apparent she had not ever done so. I did not have a sense children intentionally hid their non-compliance with rules during the interview, because children knew the purpose of the interview was to keep children like themselves safe from perceived threats online.

At the conclusion of the interview, we informed participants about all possible security issues regarding themselves and children that came up during the interview. Additionally, they were given a copy of a book written for teens and pre-teens about online safety, and we encouraged the children and adults to both read it.

3. APPROACHES TO SECURITY

We saw a number of different strategies used to keep children safe online. Next, I will provide an overview of the types of rules parents tried to enforce with regards to computer safety, as well as the various strategies for enforcing them.

3.1 Types of rules

The types of rules used by parents' rules can be broken into five categories. First, there were rules that explicitly prioritized PC use relative to other activities. These dealt with safety only to the extent that they limited access and thus gave less exposure to potential threats. These included things like "Do homework first," "Do chores first," "Don't stay on too long" often with a fixed time limit, being on the PC by a specific time in the morning or evening, parents being able to tell the child to get off when they think they have been on too long, and a rule that the PC can not be used on the weekend. Second, there were rules that were inherently based on trust or social norms. These included avoiding "inappropriate" or "adult" sites and telling children "don't embarrass yourself" or simply "you know what to do." Some families simply said they had no rules, and thus fell in this category only implicitly. Third, there were rules intended to protect the computer from threats, such as viruses or accessing adult content. These rules included things like not clicking on pop-ups, deleting all unknown email, leaving the computer alone until an adult can help, asking permission when using a new website, not letting children's friends use computers as a virus avoidance mechanism, and turning the computer off when not in use. Fourth, there were specific activities that were blocked because they were believed to be risky. These included instructions not to accept friends they didn't know on chat or IM, to always ask permission before using the computer, to either keep the door open or have a parent around when using a computer, and that the computer must run a parental control tool. Finally, there were specific activities that were blocked as they were viewed to be threatening. Children were told not to use specific websites such as MySpace, not to use chat or interactive games, or not to finalize online purchases without parental help. This suggests that among parents, there was a wide and inconsistent set of activities that were viewed as threatening and a variety of ways of delineating them as off-limits.

3.2 Strategies for enforcing rules

The twelve households with children had a variety of strategies for enforcing rules:

1. Households monitored children's actions without the use of technology
2. Households monitored children's actions using technology
3. Specific activities blocked using software because they are believed threatening.
4. Household did not monitor children, but talked about safe behavior and encouraged self restraint
5. Household did not monitor children, but talked about safe behavior and allowed curiosity

Households that monitored children's computer usage did so in a number of ways. First, some simply tried to stay in the same room as children (HH10, HH11, HH3), insisting that the door be left open or that the computer be used in a common space (HH9), or not networking the computer (HH7). (HH7 let the children use the non-networked computer unsupervised, and then applied an alternate supervisory technique when online). Lori's (HH10) sentiment that her child was too young to "have a range of choice" in doing potentially unsafe things online was

similar to those expressed by other parents of young children who employed this technique, so she was unconcerned about her child's computer use. Christina (HH3) had an opposite approach. She had a very active parenting philosophy and insisted on being in the same room. Here the children have to ask permission to use the PC. They were only allowed to view four children's sites unsupervised, one of which they were not allowed to type in themselves, because of a prior slight typo that took them to an adult site. If the children use Google for school, she checks all links before they click on them (she was unaware of safe-browse). All children in this category were under the age of ten.

Second, three of the households used technology to enforce rules. Two households had parents who monitored their children's browser cache (HH1&7); in the case of HH1 the children were aware of this, but we are uncertain if this is the case in HH7. The father of HH1 said his son has not clicked through porn ads recently as result of these approaches (HH1). He also has all of his children's email cced to him with their knowledge (HH1).

The third strategy was blocking specific activities that protection sites deemed threatening. For instance, HH6 used Net Nanny, a parental control and filtering application for the web, and both the mom and the child were frustrated at it blocking things it should not. Both mom and Julie knew that she could get around the NetNanny if she wanted to, but Julie said, "My parents trust me." "With NetNanny, I feel very safe," but at the same time she found it blocked her schoolwork. Julie continued, "I hate the Nanny." Mom commented that with NetNanny, it is "hard to get the level correct. What is moderate [level security]?"

The fourth strategy was one of no-monitoring and self-restraint. This approach was used by HH12 which had its computers in a public space. Dad said his only rules for the children were to be careful, and not to give out name, phone number or address. However, while his oldest daughter knew she was not supposed to provide her name online, she created an email account using her full name when her older brother helped her sign up for Google mail. She did not realize this was in essence providing her name online until the interview. Dad, on realizing this, said, "Nobody consulted me." He did not know his daughter's email was her full name nor that she had a MySpace page. Her email address is on her MySpace page, but she thought it was hidden. The oldest daughter said she was unaware of some of the types of information she was not supposed to provide.

The fifth strategy allowed for curiosity. This was employed by HH2 which had previously been home to a 17-year-old foster daughter, who was 16 when she came to live with the family, and intended to come back to live with them after a short break. HH2 employed a rather permissive parenting strategy due to the special circumstances of her living with them. Her parents let her browse adult content and download images. They believed their foster-daughter had "good common sense," so there were no computer rules, although safe use guidelines were presented jokingly (telling her to not to give contact info to strange men). She downloaded a lot of images and that they "let her have her own outlet." He explained, "She's basically grown up enough to do her own thing.... no concern about porn sites." Her foster-father felt this was not "damaging to her" or anyone else. This parenting philosophy is in line with danah boyd's research on MySpace that children congregate there as a part of coming to age, and use the opportunity to engage in socialization and develop their own identities as adults [1].

In addition to these enforcement strategies, HH7 tried to discourage children from using the internet. Kathy explains her strategy, "If you want your kids not to smoke you don't keep cigarettes in the house," and so she feels it is the same with the internet. The household rule is that for every hour they are using a "screened device" (games, TV, PC) they have to read.

Clearly there is a wide range of approaches to keeping children safe online, details of which require further study.

3.2.1 Enforcing rules across household boundaries

Mom or dad may make rules, but they have various degrees of applicability at school, friend's houses, the home of other parents who may share joint custody, or at the homes of grandparents. Parents may enforce rules differently. Children may choose not to follow rules outside the eye of parents. Or the caretaker may not have sufficient technological savvy to enforce the rules.

The HH9 provides an example of the latter. The father tried to monitor his 10-year-old daughter when she was online. When visiting her grandfather, she decided to create a MySpace page. Her grandfather was concerned when he realized she was getting email from a "strange man"—Tom Anderson. They later learned that Tom, as founder, sends everyone welcome email, but the damage was done. Consequently, they imposed new rules-- "no MySpace or Bebo for [Tammy]", and she can only use the computer in public spaces.

4. CHILDREN'S ATTITUDES

In the pilot study, we asked children directly for their opinions of their safety and security online. Children expressed behavior that was likely to put themselves at risk of identity theft and unwanted intrusions by for example strangers through social networks, but on whole they did not seem very concerned.

While in most instances parents volunteered safety issues on behalf of children, in two instances, the children themselves reported difficulties. One teen had had his MySpace password stolen and was very concerned about identity theft; this same teen's friend used his computer to visit a porn site and inadvertently downloaded a large virus. Secondly, a different teen reported being able to circumvent MSN's security logging by using Internet Explorer instead. His parents were aware of this, but nothing had been done, and was not viewed as particularly problematic.

5. DIGITAL PARENTING JOB-SHARING

From the fieldwork I learned households had different approaches for allocating security roles and responsibilities. I observed three primary approaches to computer security in these homes. Here I classify households by the approach used to secure the knowledge needed to accomplish the most technically demanding of the security tasks, those which I earlier termed traditional security concerns, and three primary approaches emerged. The first involved households in which a single individual emerged as the Security Czar, or the go-to person for computer security problems; the second included households where individuals were self-sufficient; and the third focused on those who looked outside to an extended Technology Household or to an Outside-Support Provider to meet their needs. I will refer to these household types as Security Czar Households, Self-Support Households, and Outside-Support Households respectively. Additionally, there was one household that was undergoing a period of transition between these categories. Each of these strategies to sharing computer security had different patterns surrounding security.

Here I discuss the pattern of sharing the burden of keeping children safe and security with regards to technology, and illustrate examples of problems mentioned during my interviews.

5.1 Security Czar

The first of the three approaches for households to meet their security needs were the Security Czar Households. This approach was used in HH 1, 9, 12 and 14. A key challenge for all families with children was keeping them safe online, and our five Security-Czar Households with children were similarly concerned. While Security Czars Households also employed social solutions such as proximity and an open-door policy to keep their children "safe" online, Security-Czar Households were more likely to use, or had plans to use, at least some sort of monitoring technology at the Security Czar's instigation. Examples included setting up emails to be cc'd to the parent, reading web-logs, or setting up multiple accounts so that the adult could access the child's account.

While two households did not use monitoring technologies at the time of the study, they expected to do so at some point. David (HH9), recently divorced, explicitly stated that he had "not gotten around to it," though he had discussed it with his former wife. Whereas Lashawn (SMO5) stated that while he was currently able to physically watch over his three-year-old daughter's shoulder when she was at the computer, he had not yet decided how he would handle the situation when she gets older.

Eric (HH12), Frank (HH1), and Barbara (HH14) all were currently relying on monitoring technology, which I will describe in depth next. Eric (HH12) had told his two teenaged daughters that they were not supposed to password-protect the account HH1 used a similar strategy when their foster daughter was still living with them. Javed was acting as the foster daughter's Security Czar, while Kate's usage remained independent. During the course of the interview, when it became apparent that his eldest daughter had disregarded this rule, Eric demanded that she, "take it [the password] off or tell us." Given that our interview took place within earshot of his daughters, David was reluctant to explain why he wanted access to his daughters' accounts. Earlier, however, he had commented that one has to assume that people have access to email just as postal workers have access to the content of postcards. This suggests that his insistence on open accounts was based on his perception that his daughters' computer use needed to be monitored as well as administratively maintained. Frank also engaged in extensive monitoring of his three children ages 9, 12, and 15. He had set up a very protective computing environment for all of the children, in part because the eldest was developmentally disabled. When asked to describe his feelings about his children's safety online he responded,

"you must understand...I run their mail server... and I run their web proxy server.. and I read the logs.. and every email that comes to them comes to me too... now you know, they know this... and uh, but I don't necessarily remind them, I like them to feel independent... and safe... but I am, I try to be quite vigilant..."

He added that he tries to "appear omnipotent, and until they get a little bit older that will work." Therefore, he had not only set up the household computing system to allow him to monitor all websites his children visited, the system allowed him to read all of their email.

This type of oversight has potential for violating the privacy of other household members. For instance, at one point my co-

interviewer asked to see the anti-virus software on one of the computers on the house. Frank's daughter had left a file open, causing Frank to comment as he reads from his child's open diary, "let's see... dear diary... probably shouldn't be reading that one." Later, when examining a different computer a number of web pages were open, and Frank jokes for the benefit of my tape recording "for those of you at home...when we came in kids were doing homework...bunch of web pages open...not trivial ones." Frank is entrusted not just with the care of the computer, but to not adversely affect works in progress.

Being a Security Czar means encountering open files—in this household that meant web pages needed for schoolwork or diaries, which children do not want their parents to read. In other households, the Security Czar may be a teenager performing the computer maintenance for adults, thereby encountering their parents' confidential documents—taxes, medical records, bank statement to which parents might not want their teen to have access. Being a teen-age Security Czar, as illustrated in my domestic economy work [19], may not carry the same authority as an adult in the role; the technical knowledge, however, constitutes power which can be used to confront authority. In either case, the Security Czar position appears to allow access to data which the household members may wish to retain as private and confidential.

Like Frank, Barbara was also engaged in monitoring; in addition, she relied on her daughter's feedback. On one occasion, the daughter reported that the family's teenaged babysitter ignored the children and played on the computer. Through some research, Barbara learned that the babysitter was putting suggestive pictures of herself on MySpace, which prompted Barbara to call the babysitter's mother to explain the potential risk. On another occasion, her son Oscar brought a friend over to play. While Oscar at age seven is not sexually curious, his friend of about the same age comes from a more permissive household. His friend used the computer to browse for images of "sexie school gurls." The mother caught this by browsing the cache. She never expected that from her son, but she told him firmly not to let his friend browse for those kinds of images or he would never be allowed to use the computer again.

Eric (HH12) had a technologically sophisticated son who had just left for college and was actively trying to maintain himself as Security Czar. Eric was careful to stress that while his son, David, may set up technologies such as multiple user accounts or the wireless, Eric was the one in charge of the security in the home. So when David set up the household network, Eric insisted that the network be set up with a password for security. Recently, however, Eric's friend Veronica began spending increasing amounts of time at his home, and he wanted to give her access to the network. Eric was embarrassed in that he needed to call his son to get the password. Here, even though Eric holds the role of Security Czar, he must continue to negotiate to continue to hold this dominant role as skill levels in the household change.

Security czars approached digital parenting primarily by monitoring using technology.

5.2 Self-Support Households

The second of the three ways in which households met their security needs involved computer owners in each household supporting their own computers. This approach was used by HH2 and HH7. In both of these households, care for the children's safety online was a topic the women spoke to at

much greater length, even though both men were asked the same questions which is indicative of these women's greater involvement in childcare related to computer use. Neither household used monitoring software. While HH2 did not place limits on what their foster daughter did online, they chose to protect the computer with anti-spyware software and by giving her a user account without administrator privileges which restricted her ability to download and install software while browsing adult-content online (Adult content is notoriously full of spyware).

Similarly, in HH7, Kathy uses social rather than technical means to keep her children safe online. She limits their total amount of screen time and insists on being physically present when they are online. She has deliberately chosen not to place the children's computer in the playroom on the network. This means the children can only use the Internet when in the kitchen or office, which makes parental supervision much easier. Depending on what her children are doing, Kathy might pay more or less attention; videos on YouTube, for example, increase the possibility that children will view adult content. While Kathy and her husband were both responsible for their own computers, it was Kathy who managed the children's safety online.

Whereas Security Czars, the five male and one female alike, were primarily responsible for monitoring children's activities online, women in the Self-Support Households were fully responsible for the day-to-day, computer-related childcare tasks. While the adults were each responsible for themselves, the women were, in essence, acting as Security Czars for the children by assuming primary responsibility for child-care related computing. Instead of monitoring technologies, these households relied on social means augmented by infrastructure to limit access (not putting computer on a network, or not allowing software installation).

5.3 Outside-Support Providers

The third and final way in which households met their security needs was to seek help from a source outside the household boundaries. This approach was used by HH 3, 6 10, & 11. For instance, Yan, a Chinese-American divorcee (HH6) with two young daughters, sought out and installed Net Nanny herself after learning her daughter had been approached by a stranger online and had had a bad experience. Similarly, Lisa's (HH11) motivation to ask her boyfriend to help set up a new machine was based on her concern that her son would damage her files accidentally. Once she obtained a second monitor, she planned on giving her son his own computer, but in the interim she had multiple accounts so that she could log him in separately. Lisa and Christina (HH3) also engaged in in-room monitoring strategies of the children's activities. Having outside security support still left these individuals with tasks they needed to perform themselves.

5.4 Transitional Household

The remaining household (HH8) was in a period of transition. The mother was actively negotiating among relying on her nearly ex-husband, relying on her new boyfriend as an Outside-Support provider, and becoming self reliant. This illustrates an example of how in certain cases digital parenting roles are in flux. Further it shows that the centralized nature of technical knowledge in these homes left children particularly vulnerable to security risks in the event of divorce of their parents or other such changes in domestic configuration.

In looking at these three primary approaches, there appears to be a relationship between technical knowledge and allocation of

digital parenting roles and the type of strategy used for keeping children safe online.

6. IMPLICATIONS FOR DESIGN

While there is a clear need for more in-depth research on children's security, I include a few implications for design:

- I have shown examples of the ways in which children put themselves at risk, but have shown that children themselves are largely unconcerned. This suggests effective mechanisms for communicating risk to children are vital.
- Children have needs for diaries and private spaces to reflect on their relationships with their parents and to develop peer relationships, but presently children's privacy is not taken into account in computer architectures. Typically adults with administrative access have access to all files. In Palen and Dourish's terms [17], they lack *reflexive interpretation of actions*. Further, children are trying to manage the boundary between the self and other. They may attempt to create a different sense of self for their peers versus their parents—engaging in Palen and Dourish's *recipient design*. In light of boyd's work on the Internet as a site of identity creation [1], this raises the larger unresolved question of children's rights to privacy online which must be resolved before a design that takes either a child-protection or child's right to privacy stance can be implemented. Presently, computer security accomplishes neither.
- Many very young children cannot read and cannot read technical language. Families often have computers almost exclusively devoted to children, or shared computers where children may be the only ones using the machine for long stretches of homework or game playing. While many adults we spoke to tried to tell children to come get them when security dialogs popped up, children admitted to often clicking them away, even those so young they could not read what the messages said. Though, they did recognize the pictures of logos. Security software needs to allow for children as illiterate principal users of machines; one way of achieving this is to design for networked maintenance across machines [9].
- Families have varying mechanisms for sharing the responsibility of digital parents, but at the same time household membership can change, causing reorganization of these abilities. If the household loses its Security Czar, it is left with a knowledge vacuum that may in particular jeopardize children's safety.
- Households ensure children's safety by both social and technical means, and thus security technologies must consider the larger socio-technical context of use.
- Rules are enforced from a variety of locations and by a variety of people outside the home, and as a consequence security for children must take into account the contingent and constructed notion of adult responsibility. Caretakers change as parents go out of town for the weekend or fall ill, and security solutions must allow for temporary caretaking across a range of physical and networked locations.

7. ETHICS & HUMAN SUBJECTS

This study left me deeply concerned about the state of research with children in HCI. Children are more often than not invisible in home research. At universities we often cannot get studies

with children through ethics review boards, or the difficulty in obtaining permission to work with them makes doing so undesirable, and few companies have the resources for these types of studies. Consequently, they are rarely done. Such utterly rudimentary findings like the need for security software to not assume literacy suggests that there is little understanding of designing to support children's needs. This suggests that there is a problematic lack of research on supporting children's needs for safety and security.

Additionally, there is a disturbing lack of discussion of ethics of user testing in the HCI community. At multiple points in the study we encountered novel situations the likes of which had not been discussed. First, there was the notion as laid out earlier in the paper that children might not be following their parents' rules, and that we might be put in a situation where we have to inform their parents of this to protect them. Secondly, there is the possibility that the children are at risk. If children are put in "unsafe" situations, the researcher is placed in an ethically complicated situation of balancing confidentiality with responsibilities to protect minors. (This can be further complicated by the role of social services who oversee issues of child welfare—ironically, while the child protection agencies in the US legislate many aspects of caring for children, I learned online safety is not considered in their policies.) Third, there is the issue of the children's rights. In HH1, all content sent by these children was sent to their dad without their knowledge. Children do not have clearly defined legal rights to privacy, and yet I find this practice objectionable. At the same time, as a fieldworker, I did not feel it was my place to intervene. We need to be discussing these issues within the HCI community.

This research also suggests we need to rethink the idealistic notions that parents and governments always protect children, and what that means for ethics review boards. For instance, Ben (HH1) who was not yet six years old was victim of one of the most significant breaches of security. His parents had recently undergone a difficult divorce, and his father attempted to fraudulently steal Ben's identity to purchase a home. A second example comes from HH2 where 17-year-old Mia had unfettered internet access. A few months after my interviewing her parents, and after she had returned to stay with her biological mother, I learned that her continued romantic relationship with a slightly older young man she met online had resulted in an unplanned pregnancy. In this instance one has to wonder if the unfettered access to adult pornographic forums sanctioned by her parents might perhaps have been ill-advised. Both of these are troubling real-life stories of children's safety being jeopardized, and they illustrate how parents might not always act in their children's best interest, be it intentionally or unintentionally, a realization which has clear implications for ethics boards and security research.

Williams [25] had a similar experience with government institutions not looking out for her participants who were non-English speaking Thai orphans, some of whom were infected with HIV. She was asked by the ethics review board committee to acquire government oversight. She felt strongly that such oversight would be more damaging to the children involved and rob her of her ability to act as an agent on behalf of her disadvantaged user population. Williams makes the point that governments may not take responsibility for informants in question thus may be unwilling to act on their behalf. In some cases, applying for government oversight requires access to all data collected which could jeopardize anonymity. Further, she makes the point that "ethnographic studies of vulnerable and disadvantaged populations are not politically neutral, even in

the most open political environments" and that as such "heavy government involvement will present a conflict of interest and only hinder honest reporting of our results. We wish to avoid being in a position where we will have to choose between honest scholarship and allowing the [agency] to continue to be effective advocates." We cannot assume people and institutions responsible for children always have their best interests at heart. This has tremendous implications for the process of ethics review boards, but also suggests that access to children independent of their parents and for long enough durations to build trust is necessary in some circumstances if their needs are to be adequately addressed in design. This issue is exceptionally complex, and is a topic requiring considerable discussion within the HCI community.

Recent research studies with children by danah boyd, Amanda Williams, and Marcela Christina Musgrove-Chávez and were all held up for months by ethics review boards (IRBs) [2, 15, 25]. Researcher danah boyd points to this experience as her reason for not going on the academic job market, as by working in industry she can work with children and not have her research crippled. She further argues that the practices are not set up for ethnographic studies, which only exacerbates the problem of working with children [2]. Further, boyd raises a number of points. We need to consider that ethics boards' primary responsibility is to keep universities from being censured for their research. The institution of ethics reviews are particularly challenged by ethnography due to its unstructured nature, and yet ethnography approaches are extremely useful for understanding children's cultures and the privacy security issues therein. Finally, it suggests that researchers are turned away from research with children, or are forced to do research with children in commercial settings. Each of these is a problematic issue for the HCI community to consider.

As we move into a space of technologies situated outside the home and situated in a complex web of power relationship and ethical norms, the HCI community requires a discussion of these issues of ethics and responsibility to both adults and child participants alike. We need to question if our existing research practices are turning researchers away from disadvantaged populations such as children which robs them of a voice in research and development.

8. CONCLUSIONS

In this paper I have shown that there are a host of privacy and security threats of which children are not aware. Further, I have discussed parents' strategies for attempting resolve or prevent potential threats. While I have shown that parents have a number of strategies for keeping their children safe and that some children themselves are concerned, this research has shown a wide range of ways in which the children are still vulnerable. In the 12 households I visited, I saw problems with children experiencing identity theft, harassment by strangers, inadvertently using one's full name online, and knowing how to get around security software. This is a broad set of issues, but it is troubling that so many could occur in such a small data set. It suggests that additional research is required to understand these issues, and to create designs that resolve them.

Finally, in order for this to happen, access to children as informants must be resolved such that researchers can gain sufficient access to understand how children use these technologies. The need for privacy and security research on children is acute, and we must, as a community, join together to remove the bureaucratic obstacles that are jeopardizing children's safety.

9. ACKNOWLEDGMENTS

I would like to thank Symantec for supporting this work, though the opinions expressed here are mine alone.

This work was conducted as part of my professional obligations at Symantec, and the interviews of children were conducted entirely without any university affiliation and not done under the guidance of university staff. That said, I would like to acknowledge Paul Dourish. Though he was not involved in conducting this work, his intellectual legacy, for which I am grateful, is reflected in this work.

Further, I would like to thank my former colleagues at Symantec, who assisted with this fieldwork: Christopher Bertrand, Michal Cohen, Meghan Ede, Gretchen Gelke, Markus te Grotenhuis, and Calvin Hart. Additionally, I would like to thank Peter Phinney for his assistance in championing this work at Symantec.

Finally, I would like to thank Amanda Williams, Louise Barkhuus, Morgan Ames, and Jofish Kaye for assistance in preparing this manuscript.

10. REFERENCES

- [1] boyd, danah. 2007. "Social Network Sites: Public, Private, or What?" *Knowledge Tree* 13, May.
- [2] boyd, danah. 2007. "When online friends spell danger." Retrieved March 2, 2009 from her site: http://www.zephoria.org/thoughts/archives/2007/09/22/why_i_am_not_go.html
- [3] Crabtree, A. and Rodden, T. 2004. "Domestic routines and design for the home", *Computer Supported Cooperative Work: An International Journal*, vol. 13, no. 2, p191-200.
- [4] Darrah, C., English-Lueck, J., and Freeman, J. 2001. "Families and Work: an Ethnography of Dual Career Families," Final Report to the Alfred P. Sloan Foundation <http://www2.sjsu.edu/depts/anthropology/svcp/SVCPslr.html>, 2001.
- [5] Dourish, P., Grinter, R., Delgado de la Flor, J., and Joseph, M. 2004. "Security in the wild: user strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing*, vol 8, no 6, p. 391-401.
- [6] Edwards, W. K. and R. E. Grinter. 2001. "At Home with Ubiquitous Computing: Seven Challenges," *Ubicomp* 2001, p256-272.
- [7] Grinter, R.E. and Eldridge. 2001. "M., y do tngs luv 2 txt msg?" *ECSCW* 2001, p219-238.
- [8] Grinter, R.E. and Palen, L., 2002. "Instant Messaging in Teen Life," *CSCW*, p21-30.
- [9] Grinter, R. E., Edwards, W. K., Newman, M. W. and Ducheneaut, N. 2005. "The Work to Make the Home Network Work," *CSCW* 2005, p469 - 488.
- [10] Harrison, A. 2009. "When Online Friends Spell Danger." Retrieved March 2, 2009 from BBC News Web site: <http://news.bbc.co.uk/1/hi/education/7046986.stm>
- [11] Harrison, A. 2009. "Online Safety Push for Children." Retrieved March 2, 2009 from BBC News Web site: <http://news.bbc.co.uk/1/hi/education/6982428.stm>
- [12] Kraut, R., Scherlis, W., Mukhopadhyay, T., Manning, J., and Kiesler, S. 1996. "The HomeNet Field Trial of Residential Internet Services," *CACM*, 39: p55-65.
- [13] Lederer, S., Hong, I., Dey, K., and Landay, A. 2004. "Personal Privacy through Understanding and Action: Five Pitfalls for Designers," *Personal and Ubiquitous Computing*, 8, 6 (Nov. 2004), 440-454.
- [14] March, W. and Fleuriot, C., Girls, Technology and Privacy: "Is My Mother Listening". *CHI* 2006, p107-110.
- [15] Marcela Christina Musgrove-Chávez. 2007. *IRB: Taming the Wild?* Interact. Position Paper.
- [16] Nader, L. 1964. "Up the Anthropologist: Perspectives Gained from Studying Up", *Reinventing Anthropology*, Dell Hymes ed., Pantheon, New York, NY.
- [17] Palen, L. and Dourish, P. 2003. "Unpacking "Privacy" for a Networked World". *CHI* 2003, p129-136.
- [18] Read, J., MacFarlane, S., Casey, C. 2002. "Endurability, Engagement and Expectations: Measuring Children's Fun." *Interaction Design and Children*.
- [19] Rode, J. A., Toye, E. F., and Blackwell, A. F. 2004. "The Domestic Economy: a Broader Unit of Analysis for End User Programming." *CHI* 2004, p161-176.
- [20] Rode, J.A. 2008. "An Ethnographic Examination of the Relationship of Gender & End-User Programming." (Doctoral dissertation, University of California Irvine, 2008).
- [21] Shehan, E. and Edwards, W. K. 2007. "Home networking and HCI: what hath god wrought?" *CHI '07*, p547-556.
- [22] Strauss, A. and Corbin, J. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Newbury Park, CA: Sage.
- [23] Tolmie, P., Crabtree, A., Rodden, T., Greenhalgh, C. and Benford, S. 2007. "Making the Home Network at Home: Digital Housekeeping", *ECSCW*, p331-350.
- [24] Tolmie, P., Pycock, J., Diggins, T., MacLean, A., and Karsenty, A. 2002. "Unremarkable Computing," *CHI* 2002, p399-406.
- [25] Williams, A. Unpublished letter to University California Irvine's Institutional Review Board. HS# 2008-6453: Use of Digital Images in a Community Caregiving Environment.