Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-Teen Mobile Safety

Alexei Czeskis[†], Ivayla Dermendjieva[†], Hussein Yapit[†], Alan Borning[†],
Batya Friedman[‡], Brian Gill[*], and Tadayoshi Kohno[†]

[†] Department of Computer Science & Engineering, University of Washington
[‡] The Information School, University of Washington
[*] Department of Mathematics, Seattle Pacific University

ABSTRACT

An increasing number of high-tech devices, such as driver monitoring systems and Internet usage monitoring tools, are advertised as useful or even necessary for good parenting of teens. Simultaneously, there is a growing market for mobile "personal safety" devices. As these trends merge, there will be significant implications for parent-teen relationships, affecting domains such as privacy, trust, and maturation. Not only the teen and his or her parents are affected; other important stakeholders include the teen's friends who may be unwittingly monitored. This problem space, with less clear-cut assets, risks, and affected parties, thus lies well outside of more typical computer security applications.

To help understand this problem domain and what, if anything, should be built, we turn to the theory and methods of Value Sensitive Design, a systematic approach to designing for human values in technology. We first develop value scenarios that highlight potential issues, benefits, harms, and challenges. We then conducted semi-structured interviews with 18 participants (9 teens and their parents). Results show significant differences with respect to information about: 1) internal state (e.g., mood) versus external environment (e.g., location) state; 2) situation (e.g., emergency vs. non-emergency); and 3) awareness (e.g., notification vs. non-notification). The value scenario and interview results positioned us to identify key technical challenges – such as strongly protecting the privacy of a teen's contextual information during ordinary situations but immediately exposing that information to others as appropriate in an emergency – and corresponding architectural levers for these technologies.

In addition to laying a foundation for future work in this area, this research serves as a prototypical example of using Value Sensitive Design to explicate the underlying human values in complex security domains.

Categories and Subject Descriptors

J.7 [**Computer Applications**]: Computers in Other Systems—*Consumer products*

Symposium on Usable Privacy and Security (SOUPS) 2010, July 14–16, 2010, Redmond, WA USA

General Terms

Security, Human Factors

Keywords

Safety, security, privacy, parenting technologies, Value Sensitive Design, value tensions, value dams and flows, direct and indirect stakeholders, maturation, teenagers, mobile phones

1. INTRODUCTION

Perhaps no issue touches the core of society as much as the raising of children. While there may be considerable disagreement about what constitutes good child-rearing, most parents seek to support their children's healthy social development and to keep their children safe from harm. Important for the work reported here, two technological trends could have significant implications for parents and their children. The first entails the development of "high-tech remote" parenting technologies that allow parents to monitor their children's activities from afar; the second entails mobile phone safety applications that take advantage of the widespread use of mobile phones to improve a person's physical safety. As these two trends merge, parents will be positioned to monitor their children's activities through the use of mobile phones, motivated in part by a desire to help keep their children safe.

To provide a flavor for these technologies, consider some that are recently on the market. Young children can be monitored via GPS jackets [38] and key rings [6], teens via in-car cameras that record their behavior while driving [11]. New mobile phone applications set off warnings when the phone enters an area deemed "unsafe" as inferred from recent police incidents and registered sex offender databases [35]; other applications allow users to photograph their surroundings in case something untoward happens, at which time the photographs would be released to the police [32]. Thus, industry has begun to market novel mobile technologies that monitor youth with the stated goal of improving their physical safety.

Those developing and deploying mobile phone parenting safety technologies face difficult challenges in determining what solutions and feature sets to implement. For example, should such technologies monitor youth surreptitiously, reporting information about a youth's activities to parents without the youth's knowledge, or should youth be aware when information about their activities is provided to their parents? What type of information about the youth should be collected? Anything that can be sensed, including emotions as well as location? Or are there some types of information that technologies should not collect? And who should have

access to this information and under what circumstances? The parents only? The parents of the child's friends? Or in an emergency situation, perhaps also the emergency responders? And perhaps other parts of the government? Who should decide? The parents? The youth? The technologists?

If technologists are to build appropriate mobile phone parenting safety technologies, then these and other complex questions need to investigated in a principled and thoughtful manner to inform the technical designs. However, this problem space lacks many of the characteristics typical of security situations. In lieu of well-defined assets, such as funds in a bank account, what is at stake here may be parenting goals such as supporting trust and maturation, which may at the same time be in tension with another important parenting goal, that of physical safety. Similarly, the relationship among actors may be less clear-cut. At times risks may arise from poor judgment by youths themselves and their friends, in addition to risks such as those resulting from emergency situations or unsavory perpetrators. Given this complexity, we approach the problem space with existing and novel techniques from Value Sensitive Design, augmenting traditional methods used in security analyses such as attack trees and threat modeling. At the broadest level, our goals are to develop new methods, approaches, and technical solutions for reasoning about security when it comes into tension with other important human values such as safety, trust, human development, and privileged relationships like those between parents and their children.

To gain traction on these issues, we conduct our work with teens and their parents. Teens represent a particularly interesting population with whom to explore the challenges of mobile phone safety parenting technologies. They are establishing independence in thought and action from their parents, demonstrate at times good judgment and at times risky judgment about people and situations, and increasingly use mobile phones under their own control in their daily lives.

Our paper is organized as follows. First, we provide background on current parenting technologies for teens, relevant work on sensing and security, and key aspects of Value Sensitive Design that inform our research approach. Next, we develop three value scenarios as a way to convey the complexity of actors, assets, and relationships involved in these technologies. We then report on a study with 18 participants (9 teens and their parents) that investigates their views, values, and priorities around mobile phone safety technologies. Taken together, the value scenarios and empirical results position us to offer design guidelines and technical directions, including recommendations for types of data to collect (or not collect), types of data to reveal to whom and when, what notification technologies need to be in place, and meaningful ways in which security mechanisms such as cryptography can be applied to data protection, retention, and sharing.

2. BACKGROUND

2.1 Parenting Technologies for Teens

Current parenting technologies for teens primarily provide parents with the ability to monitor a particular aspect of their teen's life. For example, one set of technologies focuses on monitoring and limiting a teen's online activity [1, 31, 37]. Many provide parents with the ability to record computer activity, block certain web content, or notify parents when a "sensitive" term appears on a page visited by their teen.

An additional popular trend for parenting technologies focuses on teen drivers. Some systems [30] provide parents with real-time location and speed of their teen driver. Parents can also be alerted if the vehicle exceeds a particular speed or leaves a certain geographic region. Another system [11] uses in-car cameras to monitor teens as they drive. The cameras continuously record activity inside and outside the vehicle. If the system senses a strong acceleration change (e.g., rapid breaking, a crash, rapid acceleration, swerving, or hitting a bump or curve), a process is triggered whereby a segment of video (containing activity before and after the trigger) is uploaded to a server and reviewed by an employee. If it is deemed important and appropriate, the employee forwards the video to the teen's parents along with coaching advice. The parents are then urged to speak with their teen regarding the problematic driving practices and how to improve.

Preliminary research has been conducted on the use of mobile phones as a parenting technology. However, these works differ significantly from our focus. For example, Marmasse et al. [26] consider a system for keeping track of a very young child; they did not perform any user studies or system evaluations. Yang et al. [39] conducted a broad study across many different families and social classes with children in the K-12 education system. They conclude that technology can support family communication, but they do not explore how it might do so, in which situations, or provide examples of particular applications and the related value implications.

Some parents strongly favor these types of technologies. They view the technologies as empowering, useful tools for staying in-touch with what their teens are doing. Others perceive these technologies quite negatively. For example, some educators state that preemptively monitoring teens without cause can actually worsen relationships by adding unneeded stress and demonstrating, through these actions, a lack of trust and a desire for control [9]. Many parents express concerns about being "helicopter parents," (i.e., constantly hovering over their teens), on grounds that this behavior would impede their teen's abilities to develop independence, decision making skills, and common sense [36].

2.2 Related Work in Sensing and Security

Significant research is being conducted elsewhere for sensing information from a mobile phone, such as [29]. These efforts tend to focus on using sensed information to enhance user activities. Future mobile phone parenting safety applications could use the results of such research to infer context; we do not explicitly study the methods to do so here.

Many mobile phone parenting safety applications could reveal a teen's past or present location to his or her parent, and there have been a number of key results in the field of location privacy for ubiquitous computing e.g., [3, 12, 19, 20, 23, 33]. For mobile phone parenting safety technologies, however, we envision the potential sharing of additional types of contextual information: a teen's phone may send to his or her parents the names of nearby teens, photos from the phone, and so on. We also wish to study the sharing of such contextual information explicitly in the framework of parenting and safety, with the potential interaction with other stakeholders such as the teen's friend's parents and emergency responders.

2.3 Value Sensitive Design

Originally developed in human-computer interaction [14] and since extended to ubiquitous computing [16], human-robotic interaction [22], simulation [8], and computer-

supported cooperative work [27], Value Sensitive Design (VSD) is an established approach for addressing human values throughout a technical design and implementation process. Early work in VSD engaged usable security of web browsers [28], invoking the design principle of "informing through design" [15]. Central to its practice, VSD engages conceptual investigations of key stakeholders and values, empirical investigations with actual or potential stakeholders and contexts-of-use; and technical investigations with features, architecture and infrastructure of the technology under examination and development. These three types of investigations underlie and inform our work.

Given the complexity of issues, stakeholders, and value tensions surrounding mobile phone safety technologies for teens and their parents, we drew explicitly on four aspects of VSD to investigate key values and design implications:

Direct and indirect stakeholders. Prior work in VSD [2] shows the need to consider not only the people directly interacting with technology (e.g., a person in an inside office benefiting from a web cam onto a local outdoor plaza), but also others whose data or presence may be implicated by the technology (e.g., the privacy and security of those walking through the plaza in focus of the web cam). The former are direct stakeholders of the system, the latter indirect stakeholders. In our work, we identified the teens and their parents who use the mobile phone safety applications as *direct stakeholders*. Novel for this type of research, when information about the teen's friends could also be sensed or inferred, we identified the teen's friends and their parents as one important group of *indirect stakeholders*. Recognizing that a teen might be comfortable using the technology (in a direct stakeholder relationship to the technology) but less so with a friend's use (being in an indirect stakeholder role to the same technology), we investigated priorities and design implications from both perspectives.

Value tensions. Given the complexity of parent-teen relationships and the inherent challenges of parenting an adolescent, we did not expect our design and technical work to resolve these complexities as much as to identify and engage relevant value tensions [10, 27]. As highlighted earlier, parents, in general, both want to keep their teens safe as well as support their teens' maturation. Likely teens want the same, though there may be important differences of degree and judgment. How to support these goals with technology is not at all straightforward. We anticipated the mobile phone safety designs would need to explore tensions in the perspective of both parents and teens around who has control over information about the teen and under what circumstances.

Value scenarios. Surfacing stakeholder perspectives, value tensions, and implications of potential technical solutions in a meaningful yet manageable way can be challenging. Value scenarios [34] is one VSD technique for envisioning the effects of proposed technologies when parameters of the design context are still forming and less is known about priorities and the relative importance of key assets. Value scenarios comprise fictional vignettes that emphasize social and value implications of a "hypothesized" technology. A few rich, nuanced scenarios can help to focus attention on indirect as well as direct stakeholders, nefarious and unusual uses, value tensions, and longer-term societal implications that might otherwise go unnoticed.

Value dams and flows. Value dams and flows [10, 27] is a VSD technique for identifying reasonable value-sensitive design solutions among a range of possible designs and technical features. With this technique, options that are disliked by a threshold percentage of stakeholders are removed from the design space (dams); then within the remaining design space, options that are liked by many stakeholders are identified as good candidates for the design solution (flows). In our work, we adapt the value dams and flows technique to identify what data to collect (or not collect) and, of the collected data, what to reveal to whom and under what conditions.

3. ENVISIONING PARENT-TEEN MOBILE PHONE SAFETY

We began our work with the development of numerous value scenarios to gain traction around the complexities for security decisions surrounding parent-teen mobile phone safety technologies. Here we describe three such scenarios for purposes of illustration. Each scenario highlights a set of stakeholders, contexts, and potential security and other societal concerns. Although fictional, the scenarios are grounded in actual products and events.

Value Scenario 1: Feeling safe and self-assured

Mobile parenting technology. *uSafe* is a hypothetical mobile phone application and free service developed to collect and store potential evidence and forensic information. Once installed on a mobile phone, *uSafe* allows the user to send text messages and photographs to a *uSafe* server. In turn, *uSafe* retains this information for six months and will only release it under a court issued warrant. Without a warrant, even users cannot access or inspect the information they have sent to a *uSafe* server.

Scenario. Fifteen and self-assured, Naomi is thrilled with the feeling of independence that comes with starting high school. She spends her days in a flurry of classes and extracurricular activities, with soccer practice, oboe lessons, and acting at a local theatre keeping her busy after school. Her schedule often means she is away from home until evening or sometimes after supper, but she manages to coordinate transportation without relying too much on her parents. Her older friends at school offer to give Naomi rides back and forth, and when she isn't accepting rides, she likes to walk, ride her bike or take the bus. Naomi's parents are happy that their daughter has made a smooth transition to high school and is responsibly taking charge of her own life, but they are having a difficult time with seeing less of Naomi and keeping track of her whereabouts.

One evening, Naomi leaves a play rehearsal after dark and decides to take the bus to the mall, where her friends have gathered to eat pizza and see a movie. Naomi's parents have given her the OK to do so, and are aware of which bus she is taking. During the bus ride, a strange man stares at Naomi. When she gets off of the bus at the stop by the mall, the man does also. She gets the uncomfortable feeling that he is following her, but isn't sure what to do about it; he is not overtly threatening and she feels she cannot call the police just to report feeling unsafe. She makes it to the mall without any incident, but has been frightened by the thought of being in danger. When she gets home later that night, Naomi recounts the story to her parents, who are understandably concerned. Neither Naomi nor her parents want to curtail her activities or her freedom; there have been no problems until now

and Naomi has been managing her schedule well otherwise. Naomi and her parents wonder if there could be some lightweight way that she could signal them if she found herself in over her head, before a true emergency situation arises.

Naomi's mom sees *uSafe* featured on the evening news. It sounds like just the thing to provide some peace of mind. So she proposes *uSafe* to Naomi. Naomi likes it too – especially the fact that the *uSafe* design puts notification under her control. Naomi feels like she now has a way to keep in contact with her parents without sacrificing any of her freedom or autonomy. She can use *uSafe* when she feels the need and she doesn't have to feel as if her parents are monitoring her unnecessarily.

Discussion. The *uSafe* scenario offers an example of how a mobile phone application might be used by teens and their parents as an alternative method for monitoring teen safety. Use of the application is initiated by the teens themselves and doesn't ask them to sacrifice any of their independence or for parents to violate their teen's sense of autonomy by overly-scrutinizing their activities. The *uSafe* scenario also portrays a situation in which technology is intended to be used to help protect someone's safety prior to their notifying law enforcement, with the goals of making it possible to respect the rights of others (who may or may not be acting with criminal intent) while also making the user feel more secure. More generally, it seeks a solution for a problem regularly faced by teenage girls (and women more generally), namely situations in which they feel unsafe but that aren't yet problematic enough to notify the police.

Although *uSafe* may not be the perfect solution – in fact, we have a number of concerns with it – it does raise issues that must be considered since applications like *uSafe* are already in use.

Value Scenario 2: One dad's dilemma

Mobile parenting technology. *PhoneTracker* is a hypothetical mobile phone application and website designed to help parents keep track of their teens. Once installed on a mobile phone, parents can use the application to surreptitiously turn on the phone's microphone or to read text messages on the teen's phone at any time (by logging into a webpage).

Scenario. Paul puts a great store of trust in his 14-year-old son Ben. He's been raising Ben in a suburb of San Jose, California since Ben's Mom passed away six years ago. They talk to each other a lot: share baseball, play music, take canoe trips. Although they are very close, things have changed a bit since Ben entered high school a few months ago. Ben hangs out with friends more, communicates less, and generally spends less time around the house. Paul misses the connection with Ben but figures this is normal for a teen. After all, teens need their privacy and space from their parents.

At Paul's work, talk of "life with teens" is common conversation. Several of Paul's coworkers have been telling tales: they suspect their teens of experimenting with drugs, notice alcohol on their teens' breath, and reckless driving. Last week, Betty bragged about a mobile phone app her husband had secretly installed on their daughter's cell phone: *PhoneTracker*. Now Betty knows where her daughter is hanging out, with whom, and what they're talking about. From reading text messages on her daughter's cell phone, Betty got a tip that the party planned for Saturday night would be pretty rough. So Betty planned a family gathering for Saturday night and "nipped that one in the bud". In no uncertain terms, Betty told Paul that in this day and age, any parent who isn't using a tool like *PhoneTracker* to keep tabs on their teens is being a negligent parent. Downright irresponsible. And, irresponsible not only with respect to their teen but also with the other teens involved.

At first Paul is appalled that Betty is "spying" on her daughter. But over time, pressured by Betty's stories as well as her comments that he is oblivious and naïve, Paul begins to question his own judgment as a parent. He secretly installs *PhoneTracker* on Ben's phone. Over the next several months, Paul checks Ben's activities regularly. Paul notices no discontinuities between Ben's stories and what *PhoneTracker* reports. Paul also develops a good sense of whom Ben hangs out with, where they go, and how they spend their time. It's a funny but comforting sort of communication. To his surprise, Paul also learns a great deal about Ben's best friend Jon. Things Jon's parents probably don't know. Paul wonders about that – is he spying on Jon too? Is he obligated to tell Jon's parents? How would he feel if Jon's parents were watching Ben in this way?

Then the whole thing fell apart. One evening, while Paul was checking Ben's activities on *PhoneTracker*'s website, Ben came up behind him. Ben saw what his father was looking at. Ben went ballistic – storming out of the house, shouting that Paul does not trust him. The next day, Ben threw his phone away and clams up. He's mad and sullen. Somehow, Paul's and Ben's relationship is never quite the same

Discussion. The *PhoneTracker* scenario provides a vision for how a mobile phone tracking and context monitoring application might influence the lives of direct stakeholders (teens and their parents) as well as indirect ones (the teen's friends and those friends' parents). While providing some comfort for parents and an odd sense of connection, values such as trust and respect appear to be eroded as the technology easily allows parents to watch their teens unnoticed. At its broadest level the scenario points to the possibility for far-reaching changes in societal expectations and norms around what constitutes good parenting.

Value Scenario 3: "Accidental" data

Mobile parenting technology. *RoadGuardian* is a hypothetical car-based system and service designed to monitor and support safe driving by teens and other new drivers. Within the car, the system includes sensors that can detect sharp turns, sudden braking, and large bumps, along with an internal and external camera; when the vehicle makes a sharp turn, brakes suddenly, or hits a large bump, the cameras record short video clips of the interior cabin and front of the car. These video clips are then sent to a server where a *RoadGuardian* employee reviews the content. Per corporate policy, only videos that the employee determines indicate unsafe driving are forwarded to parents; other videos must be deleted. In addition, if the employee detects an accident, emergency responders may be contacted.

Scenario. Tiffany has just celebrated her 16th birthday with what she considers as "the greatest present of all": a driver's license. She's excited by the prospects for independence and the chance to control her own schedule. No more begging her parents and her friends' parents for rides. Tiffany's parents greet this change with mixed feelings; they are pleased to see their daughter growing up and experiencing new self-determination, but at the same time, they're nervous about Tiffany's judgment, her inexperience as a driver, and

the dynamics of teens and cars. They agree that Tiffany can have use of the family car on the condition that she uses the *RoadGuardian* system – that way, they'll get a heads up if Tiffany's driving is getting out of hand and can take steps accordingly, especially before an accident happens. Although she feels a little uncomfortable with being monitored, Tiffany agrees to the condition; it seems a small price to pay for the freedom that comes with being able to drive herself around. *RoadGuardian* is installed in the family car and activated by proximity to a fob on Tiffany's key chain whenever she's behind the wheel. After awhile, Tiffany forgets that the system is installed and gets into no hazardous situations while on the road; her parents are pleased that she is proving to be a safe and responsible driver.

Tiffany and her best friend Ashley are on the high school cheer squad, and Tiffany often drives with Ashley to practice at the nearby football stadium after school. One day after cheer practice, the girls decide to treat themselves to a cup of hot chocolate at a local coffee shop. Tiffany finishes her drink before getting in the car to drive and Ashley takes her drink with her. During the ride, the lid comes off and the hot chocolate spills on Ashley's shirt. She puts the drink down in the cup holder and reaches into the backseat to grab another t-shirt from her bag. Just as Ashley is in the middle of swapping tops, Tiffany hits a speed bump while going too fast, her attention having been momentarily drawn away from the road because of the hot chocolate spill. Registering the jolt, the *RoadGuardian* system takes a short video of the cabin of the car, capturing Ashley in the process of changing clothes and Tiffany not watching the road.

This video clip is later examined by Jeff, a *RoadGuardian* employee, who has only been on the job for six months and has not had to make any difficult judgment calls on what incoming data should be kept and sent to parents. Corporate policy is that only images of the teen driving unsafely should be forwarded to parents, and that other images (such as pictures of the teen in revealing positions) should be deleted. In the video clip from Tiffany and Ashley's afternoon, Ashley is seen partially undressed, even though Tiffany appears to be driving somewhat unsafely. Jeff makes the call to not forward the data in order to protect Ashley's privacy, given that no accident resulted from the situation, but not to delete it.

However, several months later, while watching funny videos online, Ashley's brother discovers a clip of his sister in Tiffany's car – the same clip taken by the *RoadGuardian* device. He finds it hilarious and shows it to Ashley immediately, who is horrified and embarrassed. She had no idea that a video camera was installed in Tiffany's car, nor was she aware that the images would be sent to a third-party company. She feels as if her friend tricked and betrayed her somehow. It turns out that someone hacked into the *RoadGuardian* system, and data that was supposed to have been deleted was leaked onto the internet.

Discussion. This is an example of a system that monitors the state of a car and records its interior and exterior during unusual events in order to foster safety and improve a teen's driving skills. The process used by *RoadGuardian*'s employees to screen the recorded content before it is sent to the parents can have multiple uses – for example, if there is an emergency, they can alert the emergency responders. Additionally, they can analyze the situation and reduce potential false alarms (e.g., a bump in the road and not a crash). However, the ability for a stranger to look at this content creates additional complications. For example, what if the video contains images of a sexual nature and the participants are underage – does this qualify as child pornography? What if the employee mishandles the recordings? Finally, as modeled by this scenario, this system has the ability to not only negatively impact the direct stakeholder, who is aware of its existence, but also indirect stakeholders (others who are riding in the car and might not even be aware of the system).

4. PARENT-TEEN PERSPECTIVES ON MOBILE PHONE SAFETY

The value scenarios go a good distance toward surfacing complexity in parent-teen mobile phone safety technologies. As a group, the scenarios point toward issues of trust and maturation, raise questions about what sort of data should be sensed and who should have access to it and under what conditions, impacts on indirect stakeholders, and the risks from third parties leaking information, either intentionally or unintentionally. What the scenarios cannot tell us is what actual parents and teens, living in relationship together, think, experience, and value in these situations. For that, we must turn to other methods: namely those that engage real parents and their teens in the context of these envisioned technologies.

Toward that end, we conducted semi-structured interviews with 9 parent-teen pairs about their views and values in relation to mobile phone safety technologies for teens. This section reports on our interview methods and key results.

4.1 Methods

4.1.1 Participants

Eighteen participants, 9 parent-teen pairs (5 sons and their mothers; 2 daughters and their mothers; and 2 daughters and their fathers) participated in this study. Parents' average age was 53 (median = 51; range = 48-59); teens' average age was 15 (median = 15; range = 14-17).

Participants were recruited with flyers posted in local public schools and community centers, as well as with online postings to electronic message boards. Parent-teen pairs who would respond to such a solicitation likely have reasonably positive relationships, as both had to agree to participate.

4.1.2 Interview Logistics

Interviews were audio-recorded and lasted approximately an hour-and-a-half. To protect the privacy of each participant's responses and to avoid interviewer bias, teens and their parents were interviewed in separate rooms by different interviewers.

4.1.3 Interview Structure and Questions

Semi-structured interviews contain a set of specific questions asked of each participant but allow for follow up questions and conversation to tap the issues of interest to the participant. The interview consisted of four sections: two introductory sections, one on general considerations of parenting and personal experiences, and one reflecting on current technology to improve personal safety. These were followed by the core of the interview, a detailed investigation of an envisioned mobile phone safety technology for teens. The last section briefly considered abstract values of potential import. We describe each section in turn.

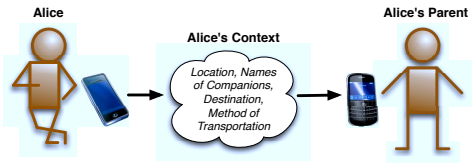

Figure 1: Direct Stakeholder Role. Illustration of the type of mobile phone safety system participants were asked to envision: Teen Alice has a smartphone that recognizes certain aspects of her context and then sends that information to her parent under certain conditions.

General Views on and Personal Experiences with Parenting. We began the interview with broad questions to tap participant's general views on and personal experiences with parenting (e.g., need for a curfew, involvement with homework), the purview of a teen's activities (e.g., are there things in a teen's life that you consider private and would not want shared with a parent), and with unsafe situations (e.g., how frequently do you think your teen is in an unsafe situation). These questions provided important context for the remainder of the interview and alerted us to past dangerous situations the teen might have experienced.

Current Personal Safety Technology. Next, we asked participants about three current commercially available technologies designed to improve user safety: in-car monitoring system for teen drivers [11], computer use monitoring software that record keystrokes, sites visited, emails sent, and other information (e.g, [1, 5, 31, 37]), and a user directed application for recording and storing context information in potentially threatening situations [32]. For each type of technology, we asked participants how they felt about its use in the context of parenting (e.g., should parents of teens use this technology; if parents use this technology, should they tell their teens that they are doing so). These questions provided insight into the values that may be impacted by safety technologies, grounding abstract concepts such as autonomy, trust, and privacy in particular systems and contexts of use.

Feature Evaluation for an Envisioned Mobile Phone Safety Technology. The bulk of our study focused on exploring possible features of several classes of envisioned applications. Specifically, we investigated what types of context data about the teen's activities (e.g., where the teen is or what the teen is doing) should be made available to various parties such as parents or emergency responders, and under which (if any) circumstances.

Participants were asked to envision a system in which the teen has a smartphone that can determine certain aspects of the environment and relay that information to another party. Initially, we asked participants to take the point of view of a direct stakeholder (e.g., a user of the system). That is, the teen was asked to imagine that his or her smartphone sensed data about him or herself, and could make that data accessible to his or her parent. Analogously, the respective roles were described for the parents as well. (See Figure 1).

Once participants understood the technology, we then asked them how they felt about this system while carefully varying features along the following three dimensions:

a) **The type of information being sensed.** The collected information can be grouped roughly into information about the external environment and the teen's internal state as follows:

- *External environment.* Teen's location, names of companions, destination, and type of transportation.
- *Internal state.* Teen's mood.

b) **The recipient of the information.** The various recipients were the teen's parents, the teen's friends, emergency responders, and the government.

c) **Under one of three conditions:**

- *No awareness.* Teen would not be notified when a party (their parents, friends, emergency responders, or government) accessed his/her context information.
- *Awareness.* Teen would be notified via a pop-up on his/her phone that a party had requested his/her context information.
- *Dangerous/Emergency Situation.* The phone has recognized some dangerous or emergency situation, and can contact various parties about this situation as well as provide the teen's context information.

For each combination of the above, participants were asked to indicate whether they wanted the teen's information to *always*, *sometimes*, or *never* be shared. Because of the large number of permutations and to provide participants with the opportunity to review and compare their own responses, we presented the combinations to participants in the form of a large chart. Participants indicated their evaluations (i.e., always, sometimes, never) for each cell in the chart (corresponding to a different combination) with a colored marker. Thus, the pattern of the participant's responses became visible as the participant worked through the various information types, recipients, and conditions.

After teens and their parents had considered the technology from the point of view of using the system, we asked them to assume the role of indirect stakeholders. Specifically, participants were told that if one of the teen's friends had this type of smart phone, then whenever the teen spent time with that friend, information about the teen would also be collected and transmitted to the teen's friend's parents (see Figure 2). We then asked participants to reconsider their responses along the three dimensions as they imagined themselves in the indirect stakeholder role. Again, participants were asked to indicate whether they wanted the teen's information to *always*, *sometimes*, or *never* be released. A similar chart was used to capture and record the data.

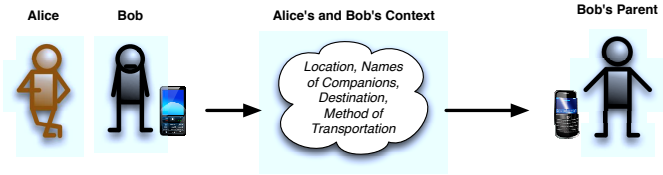

Figure 2: Indirect Stakeholder Role. Illustration of the same mobile phone safety system, with teen Alice as an indirect stakeholder: Alice's friend Bob has a smartphone that reports a part of his context to his parent. Whenever Alice is with Bob, Bob's parent will be able to know various information about Alice.

Values Rating Activity. Finally, we were interested in understanding on a more general level what values participants consider more important when reflecting on mobile phone safety technologies with teens. We first identified a list of 14 likely relevant values by drawing on prior literature and

on our value scenarios. Then we asked participants to sort each of these values into one of three piles: *1) care about a lot*, *2) care about somewhat*, and *3) not that important*. The appendix provides a list of these values and the definitions we provided to participants. As appropriate, value definitions were adapted to reflect a parent or a teen perspective.

4.1.4 Coding and Reliability

Interviews were transcribed for coding and analysis. Each interview resulted in an average of 46 transcribed pages.

A coding manual was then developed first from all of the interviews. As part of that coding manual development, systematic criteria were developed for how to handle border cases. Then two researchers trained in the coding manual independently coded all of the data. Inter-coder reliability was assessed using Cohen's kappa[1], with $\kappa = 0.724$ for the interview questions reported in this paper.

4.1.5 Data Analysis

Data were analyzed as follows:

- **Within group.** This type of analysis is performed on the group consisting of just teens or the group consisting of just parents. These are within subject *matched-pair* analyses involving comparisons of a participant's responses to one question against the same participant's responses to other questions.
- **Inter-group.** This type of analysis compares the teen group to the parent group. Such analyses are also matched-pairs analyses in which each teen is compared with his or her own parent.

Because the data are purely ordinal, nonparametric tests are used for all statistical comparisons. Since all tests involve matched-pairs, Friedman's test is used when comparing three or more variables and Wilcoxon's signed-rank test is used when comparing two variables.

4.2 Results

The semi-structured interviews generated a large amount of qualitative and quantitative data. Due to space limitations, we report on aspects most relevant to informing design and setting the technical direction for mobile phone safety technologies for use with teens.

4.2.1 General Views on Teen Privacy

To situate our results on mobile phone safety technology, we first provide a sense for how teens and their parents view teen privacy. We focus on why teens don't share certain types of information with their parents, why some parents agree with this decision, and one misconception that both teens and parents have about each other regarding information sharing. We analyze these in the context of social and location data and communication through electronic media like Facebook.

Among our participants, all but one teen indicated that there are parts of their lives that they would not want to share with their parents. Commonly, the teens felt shy sharing events that they considered to be embarrassing, such as information about boyfriends or girlfriends. Parents expressed understanding about this being a personal topic, as one parent stated:

> "... anything to do with his friendships that he feels or girlfriends ... anything he thinks is private I would respect as private."

A popular trend we observed among roughly half (five out of nine) of the teens we interviewed is their use of technology to interact with friends, most notably Facebook. Three out of those five mentioned that they have written something on their Facebook pages that they do not want their parents to know/see. As one teen suggests:

> "... it would just be kind of weird if I was Facebook friends with my mom and knowing she could just go on my profile and see what I write on people's walls or like, like ... talking about hot celebrities ... like I don't talk to my parents about that."

This quote suggests (also shown in [4]) that teens do portray a different image to the different people in their lives. Some parents view this as a natural part of the maturation process. One parent speculated that the things her son might write in his Facebook profile are:

> "... things that reveal who he is to his friends or the image of himself that he wants to create to his friends that has nothing to do with me. It's all his own ... it's more about just trying to have his own identity, which is very appropriate at this age."

For teens, the desire for privacy also manifests itself in teens' daily activities: six out of nine teens have told their parents they were in one location, when they were in another. However, the teens stated that reasons for this are actually mostly due to laziness, for example when the teen might be in transition from one place to another or inconvenience of always having to check in when changing locations. Whatever the reasoning, parents seem to be mostly unaware of this; only two of the nine parents could recall a time when teens had told them they were in one location when they were in another.

4.2.2 Mobile Phone Safety Technology

We now turn to the substance of our analysis of how parents and teens might use a mobile phone safety technology as described in Section 4.1.3. We focus on the sharing of information from each category of potentially sensed data: *exact address*, *destination*, *names of companions*, *transportation type*, and *mood* – and examine how participants want each type of data shared with each stakeholder (teen's parents, teen's friends, emergency responders, and government).

Type of information sensed: External vs. internal. We expected both teens and parents to be more reluctant to share information about internal states than information about external environment. Results showed that four out of the nine parents and three of the nine teens said that *mood* should never be shared with anyone under any circumstances. Many participants referred to mood as "too personal" to be automatically shared. One parent also went to note that checking his teen's mood "is just morally wrong". In contrast, all

[1]Cohen's kappa is a measure of the level of agreement between two coders. Two commonly referenced benchmarks for interpreting the values of Cohen's kappa are Fleiss [13], who rates any value of κ over 0.75 as excellent agreement, between 0.40 and 0.75 as intermediate to good, and below 0.40 as poor; and Landis and Koch [24], who rate a κ of 0.81 to 1.00 as "almost perfect" and between 0.61 and 0.80 as "substantial" agreement.

nine teens were willing, at least under some circumstances, to share information about their *exact address*, *names of companions*, *transportation type*, and *destination*. Similarly, all nine parents felt that under some conditions it was appropriate to share information about *exact address*, *names of companions*, and *transportation type*; eight of the nine parents felt that it was okay under some circumstances to share information about *destination*. Following a "value dams and flows" approach in which features that are viewed strongly negatively by a threshold percentage of users are not implemented (value dams), the fact that a substantial percentage of both parents (44%) and teens (33%) felt that *mood* should never be shared indicates that this is a design feature that should be avoided (i.e., *mood* should not be collected).

Therefore, mood is not included in the remaining results in this paper. All subsequent scores are computed based only on the questions regarding external environment.

Notification and awareness. We also expected that teens would be more willing to share information under the condition that they would be notified when a party accessed that information. To obtain an overall measure for how willing parents and teens were to share information under each condition, we computed scores for each participant as follows: each response (*always*, *sometimes*, or *never*) was assigned a score of 2, 1, or 0 points, respectively. For each of the three different conditions (no notification, with notification, and emergency), we then computed a total score by adding up the participant's responses across the four different types of stakeholders (parents, teen's friends, emergency responders, and government) and each of the four different types of external environment information (*exact address*, *names of companions*, *destination*, and *transportation type*). Separate scores were computed for each participant for each of the three different conditions (no awareness, awareness, and emergency), yielding scores which could potentially range from 0 (never share any of the types of information with any of the stakeholders) to 32 (always share all types of information with all of the different stakeholders). For teens, total scores for sharing information without notification ranged from 0 to 29 with mean $\bar{x} = 8.7$, median $M = 7$, and SD = 8.72, while scores for sharing information with notification ranged from 2 to 31 with $\bar{x} = 13.9$, $M = 11$, and SD = 10.06. Wilcoxon's signed rank test indicates that the scores tend to be significantly higher for teens with notification than without (Z = -2.20, $p = 0.028$). For parents, total scores for sharing information without notification ranged from 0 to 4 with $\bar{x} = 0.9$, $M = 0$, and SD = 1.76, while scores for sharing information with notification ranged from 0 to 12 with $\bar{x} = 4.67$, $M = 5$, and SD = 4.67. Wilcoxon's signed rank test indicates that the scores also tend to be significantly higher for parents with notification than without (Z = -2.06, $p = 0.039$). Thus notification results in a significant increase in the acceptability of sharing information for both teens and parents, as one teen noted:

> "I'm more sympathetic with them notifying me."

Emergencies vs. non-emergencies. We also expected that teens and parents would be more willing to share information in emergencies or dangerous situations than in non-emergencies. This expectation was verified by our empirical results, as echoed by one teen:

> "In that case... like in case of an emergency like I would be OK with [sharing] like any of this stuff."

Using the process described above to create a total score for the amount of information that teens and parents thought should be shared in emergencies, scores ranged from 17 to 32 for teens with $\bar{x} = 24.3$, $M = 24$, and SD = 4.66. These total scores for the amount of information that teens were willing to share in an emergency were significantly higher than their scores for non-emergency situations, either with notification (Wilcoxon signed rank test, Z = -2.67, $p = 0.008$) or without notification (Z = -2.43, $p = 0.015$). For parents, scores ranged from 12 to 28 with $\bar{x} = 19.7$, $M = 18$, and SD = 5.79. Like the teens, parents had higher scores for the amount of information that they thought should be shared in an emergency than in a non-emergency situation, both with notification (Z = -2.67, $p = 0.008$) and without notification (Z = -2.69, $p = 0.007$).

Stakeholder	Mean	Median	Range	SD
Parent	14.0	13	10 - 24	4.87
Friends	13.3	14	6 - 20	5.41
Emergency Responders	13.1	13	6 - 24	5.86
Government	6.4	2	0 - 24	7.86

Table 1: Summary of teens' scores for willingness to share information with different stakeholders.

Stakeholder	Mean	Median	Range	SD
Parent	10.8	9	6 - 20	4.74
Friends	3.7	1	0 - 12	4.58
Emergency Responders	8.2	8	6 - 12	1.56
Government	2.4	2	0 - 8	2.83

Table 2: Summary of parents' scores for willingness to share information with different stakeholders.

Sharing information with different stakeholders. Does it matter who the recipient of the information is? To obtain overall measures for how willing parents and teens were to share information with each of the different stakeholders, we computed scores for each participant, with *always* = 2, *sometimes* = 1, and *never* = 0. For each of the four different stakeholders, we then computed a total score by adding up the participant's responses across the three different conditions (no notification, with notification, and emergency) and each of the four different types of external environment information (*exact address*, *names of companions*, *destination*, and *transportation type*). Separate scores were computed for each participant for each of the four different stakeholders (parents, teen's friends, emergency responders, and government), yielding scores which could potentially range from 0 (never share any information with this stakeholder) to 24 (always share all types of information with this stakeholder). Summaries of the scores are reported in Table 1 for teens and in Table 2 for parents.

For teens, an overall test for differences among the distributions of scores for the four different stakeholders indicates significant differences (Friedman's test; $\chi^2 = 11.205$, d.f. = 3, $p = 0.011$). Fisher's least significant difference (LSD) method applied to ranks was then used for all pairwise comparisons among the four stakeholders; results showed that teens were significantly less willing to share information with government than any of the other three stakeholders, and there were no significant differences among the scores for the other three stakeholders. As one teen pointed out:

> "I'd feel weird if I knew the government was checking on all these little situations I get myself into."

For parents, Friedman's test again indicates significant differences among the scores for the four different stakeholders

($\chi^2 = 20.734$, d.f. $= 3$, $p < 0.0005$). Pairwise comparisons among the four stakeholders using Fisher's LSD method indicate that scores were significantly lower for sharing information with the teens' friends and with government than for sharing information with parents or emergency responders.

These results indicate that both teens and parents are generally uncomfortable sharing information with government. The teens are comfortable sharing information with their friends, but parents generally do not want information shared with their teen's friends, as implied by one parent:

> "I don't want [my teen's friends] to know anything without her knowing."

Teen vs. parent responses. The design of the study also allows us to make direct comparisons between the responses of each teen and the responses of his/her own parent. Each participant was asked whether or not they would be willing to share each of the four different types of external environment information with four different stakeholders in three different contexts, for a total of 48 such questions per participant. Slightly over half of the time (55%, 236 out of 432 responses across the nine parent-teen pairs), the teen and his/her parent gave exactly the same response. In most cases when there was disagreement, the teen was more willing to share information than the parent (37%, 161 out of 432). In a small number of cases, the parent wanted information shared more than the teen (8%, 31 out of 432).

We then used Wilcoxon's signed rank test to compare teens' and parents' willingness to share information with each of the different stakeholders (see Tables 1 and 2 for descriptive summaries). Results showed that scores were significantly higher for teens than for their parents for sharing information with friends ($Z = -2.43$, $p = 0.015$), emergency responders ($Z = -2.32$, $p = 0.021$), and government ($Z = -2.00$, $p = 0.046$). These results may indicate generally higher levels of concern about privacy by parents than by teens. However, the amount of information teens were willing to provide to their parents was not significantly different from the amount of information that the parents actually wanted ($Z = -1.47$, $p = 0.141$). This last result was particularly surprising. We expected that teens would be more conservative in sharing information about their daily activities with their parents than their parents would like, but the results did not support this expectation, reflecting a high level of agreement between parents and teens. In fact, when parents and teens in our sample did disagree, the teen tended to be willing to provide more information than the parent wanted, even in the context of sharing information with their own parent.

Direct vs. indirect stakeholders. Teens and parents were also asked to imagine themselves as indirect stakeholders of the technology. That is, they were asked to consider a situation in which one of the teen's friends has the device and to assess how information should be shared by the teen's friend with the friend's parents. Total scores were computed for each participant's willingness to share information with a friend's parent in this context, and these scores were compared to their previously computed scores for sharing information with their own parents. Results showed that teens were somewhat more reluctant to share information with parents in this situation. Teens' scores for information shared with their friend's parents when they were the direct stakeholders ranged from 10 to 24 with $\bar{x} = 14.0$, $M = 13$, and SD $= 4.87$, while scores for sharing information with friend's parents when they were the indirect stakeholder were somewhat lower (Wilcoxon signed-rank test, $Z = -2.132$, $p = 0.033$), with scores ranging from 0 to 24 with $\bar{x} = 11.3$, $M = 11$, and SD $= 7.54$. However, for parents there was no significant change in scores ($Z = -0.631$, $p = 0.528$) when they were placed in the indirect stakeholder role ($\bar{x} = 12.4$, $M = 12$, and SD $= 7.54$) vs. when they were in the direct stakeholder role ($\bar{x} = 10.8$, $M = 9$, and SD $= 4.74$).

4.2.3 What do Teens and Their Parents Value?

To ensure that the technical directions we set would be responsive to issues that teens and their parents consider most important, we looked at what teens and their parents care a lot about. We were also interested in the degree to which parents and their teens shared views on what matters. Areas of agreement – particularly aspects that are of high import – would provide clear direction for technical features and design; in contrast, areas of disagreement would point to dimensions that would require further study and careful treatment.

Table 3 (in the appendix) shows the percentage of parents and the percentage of teens who said that they "care a lot about" each of 14 values. We first performed a *within* group analysis to determine if the parent group identified certain values as being more important than others; the same was done for the teen group. Each response was scored as 0 = "not really that important", 1 = "care about somewhat", or 2 = "care about a lot". Using these scores, Friedman's test indicated clear differences in importance of values both among parents: ($\chi^2 = 53.017, 13$ d.f., $p < 0.005$) and among teens: ($\chi^2 = 23.831, 13$ d.f., $p = 0.031$).

Pairwise comparisons among the 14 different values were then conducted using Fisher's LSD method. Based on the results of these pairwise comparisons, we placed each value into one of three clusters. A "most important" cluster contains values which are (1) significantly *more* important than at least one of the other 14 values and (2) not significantly less important than any values in the list. A "least important" cluster contains values which are (1) significantly *less* important than at least one of the other 14 values and (2) not significantly more important than any values in the list. All other values were put into an "in-between" cluster. We observed that for both the teen and parent groups, *safety, informed consent, trust him/her, trust you,* and *autonomy* are in the "most important" cluster. Additionally, for both parents and teens, *spontaneity, property,* and *reliance on technology* are in the "less important" cluster.

Interestingly, *false sense of security* is in the "most important" cluster for parents, but in the "less important" cluster for teens, indicating some level of disagreement over its relative importance. Indeed, a Wilcoxon signed-rank test comparing each teen's response against their own parent's response shows that the parents considered a false sense of security as more important than did the teens ($Z = -2.12$, $p = 0.034$)[2]. This suggests that teens may feel somewhat invulnerable.

[2]Out of 14 values, this is the only comparison that results in a statistically significant difference between parents and teens. Despite the large difference observed descriptively (89% of parents "care a lot" about this value vs. only 25% of teens), adjusting for multiple comparisons would render this comparison non-significant as well due to the small sample size.

4.2.4 Broader Context

The technologies reviewed, as well as the one proposed in this paper, can often have non-obvious side-effects. We explore two of them below:

Effect on Individuals. During the course of the interviews, we studied a feature that provides teens with a choice to either share or not share their information. With this feature, every time teens are queried for information, they would get a pop-up with an "Accept" button and a "Reject" button which will allow them to choose whether or not the information should be provided. Should the teen wish to reject the request, the parent will not be notified that the teen rejected, but rather they will receive a message alerting them that the information cannot be determined. This feature was met with much enthusiasm by the teens – 8 out of 9 teens said they may change some of the answers to the charts if they had such a feature.

An interesting side-effect of this design feature concerns parents who may have become accustomed to always being able to access their teen's status. They may become worried simply on the basis that this information is not available. One teen expressed how this could lead to confusion:

> "[My boyfriend's mom] would probably freak out [if the phone said that the information cannot be determined] and be like, 'why can't this be determined? Like, is there a problem? Like, is he hurt?'

Effect on Society. Our empirical investigation also found that the concern for groundless fear extends beyond the individual family unit to encompass society more generally. This became most apparent in the participants' evaluation of My Mobile Witness [32]. For example:

> "I think [technologies like My Mobile Witness] could make everyone's way of being in the world very paranoid ... [It] like would re-frame how people went through their life, in a way that I don't think is conducive to my sense of ... of a good society."

The concern is that such technologies encourage individuals to constantly be suspicious and see potential criminals or aggressors everywhere. This type of world view will not only cause stress through unnecessary paranoia, but has the potential to victimize innocent bystanders by taking pictures of everyone and thereby possibly violating their privacy. Many participants echoed this concern with respect to themselves as indirect stakeholders – they do not wish to have their pictures taken by people who they do not know without permission.

5. INFORMING DESIGN AND TECHNICAL DIRECTIONS

The above conceptual and empirical investigations have given us key insights into parent-teen mobile safety technologies. We synthesize these insights here, focusing on how they help illuminate the security and privacy landscape surrounding these emerging technologies. Given a set of specific security and privacy goals, it is often (though not always) possible to devise a system technically capable of achieving those goals. However, for comlex technologies such these, it can be fundamentally challenging to determine *what* those goals ought to be. Our conceptual and empirical investigations give us an opportunity to answer such questions. And, as a result, we also have the opportunity to make concrete recommendations for the design of future parent-teen mobile safety technologies.

Surprisingly, we found that teens in our study were largely in agreement with their parents regarding the amount and types of their information that should be shared. Even more surprising was the observation that when parents and teens did disagree, teens were often willing to share slightly *more* information than their parents requested; we did not initially expect teens to be so supportive of these technologies. These two observations suggest that parent-teen mobile safety technologies may be suitable (and even attractive) in some parent-teen relationships. Furthermore, if given the option to be notified when their parents accessed their information, the teens were even more willing to share their context information. This suggests that future parent-teen mobile safety technologies should include teen *notification*, *awareness*, and *control* principles in their design. Although others have observed the value of such notification in the past, e.g., [21], our empirical results concretely demonstrate the value of such notification in the context of our population group. We observe that notification and monitoring awareness is also supportive of safety, informed consent, and trust – several values that we previously identified as being particularly important to both parents and teens.

While our study group is not representative of all parents and teens, it does represent one realistic user base of future parent-teen mobile phone safety technologies, and hence understanding their perceptions of these technologies is valuable. Besides noting the value of notification and awareness of monitoring, there are a number of other lessons to learn from our conceptual and empirical results. In general these lessons also have associated design challenges. Central among these lessons are the following:

Inequality of data. Our results suggest that not all data are created equal. At one end of the spectrum is information that should *never* be sensed or collected: mood. Although sensing mood is feasible – and an active topic of research, e.g., [18] – a predominant number of both teens and parents felt uncomfortable about exposing a teen's mood to other parties (including to the parent). The degree to which they were uncomfortable sharing this information suggests that the information should never be sensed or collected. Not sensing the information completely circumvents the risk of having the data accidentally exposed later, either as part of a legal investigation or as the result of an attack.

At the other end of the spectrum is information that should be collected for legitimate purposes. For example, a teen's GPS location trace can prove valuable if the teen is later determined to be missing. Similarly, photos or audio recordings taken by the teen's phone – whether captured automatically or at the teen's explicit request – could prove valuable in forensic investigation or scene reconstruction.

Our conceptual and empirical results suggest that location, photos, and audio are examples of significantly different types of data. For example, GPS traces and photographs could reveal private information not only about the teen, but also others in his or her environment – the indirect stakeholders. Moreover, photos could reveal indirect stakeholders' moods – something we argued should not be collected. Hence, a fundamental question arises regarding whether or not to col-

lect this information and how to adequately protect it. We need to ensure that an attacker cannot infer mood (or other undesired information) from the collected data.

Inequity of situations. A separate and significant observation is that not all situations are created equal. Although teens and parents can be reticent to share certain classes of information with others, the willingness to share information significantly increases during emergency situations.

The differences between non-emergency and emergency situations beg the question of how to appropriately protect the privacy of data so that it is inaccessible to third parties (including government employees and the company providing the parent-teen mobile phone monitoring services) during ordinary situations, but becomes (immediately) accessible during emergencies. Additionally, we observe that emergency situations, once dealt with, become non-emergencies. The data that emergency responders needed to handle the emergency may no longer be needed after the emergency subsides, and hence their access to it should be revoked.

A separate challenge, that we do not specifically address here, is how to define an "emergency." An emergency could be defined in many ways: e.g., by the teen when the teen presses a certain button, by the police after the parent files a missing person report, or automatically if the phone detects a rapid deceleration indicative of a high-speed crash.

Inequity of recipients. A key observation – alluded to above – is that not all recipients of data are created equal. For example, teens and parents are more willing to share certain information (e.g., location) with parents than with the government. On the other hand, teens may be reticent to share photos that their phone automatically captures with their parents, but might be willing to share those photos with emergency responders if they can be assured that the information will only be accessible in emergencies. The design of a parent-teen mobile phone safety application must thus support different pathways for sharing the data collected on the teen's phone.

Avoid making coercive environments worse. Our interviews focussed on parents and teens who are in reasonably well-functioning relationships – both the parent and teen had to agree to participate. During our study, one of our participants, who had previously worked professionally with abuse victims, surfaced an important stakeholder subgroup to consider: teens who are in abusive relationships, either inside the home or out.

Teens who may be abused at home represent an important and challenging group to design for. In our current work, we make suggestions that avoid making bad situations like this worse, for example, by constantly exposing a teen's location to the parent without the teen's knowledge, permission, or control (ability to turn off). While the marketplace does have technologies that can amplify abusive parent-teen relationships (e.g., GPS tracking devices), we seek mechanisms for creating technologies that cannot be used to amplify abuse. For example, the notification and monitoring awareness mentioned earlier could help, as could allowing teens to deliberately report false information (such as the by-now folklore proposal for letting users lie about their locations when using location-based services).

Second, we must consider the possibility that a teen using the mobile phone technology might find him or herself in a coercive environment – for example, in an abusive dating relationship, or in the company of a large group of other teens that make him or her uncomfortable. In these cases, a teen might wish to "stealthily" call his/her own parent for assistance without the abusive people in his or her environment being able to observe that she's doing so and react coercively.

Avoid overburdening emergency responders. Like other technology-based services that help people with their physical safety (e.g., GM's OnStar service, which can place emergency calls when cars get in accidents or ADT's home monitoring service, which can contact police or emergency responders in the event of forced entry or fire) a parent-teen mobile phone safety technology must avoid overtaxing emergency responders with false alarms. In the case of OnStar and ADT, emergency responders are not directly contacted by the user's car or home. Rather, first the OnStar and ADT call centers are notified of a potential event and, depending on the situation, OnStar and ADT may choose to notify emergency responders. Like OnStar and ADT, there is value is placing an intermediary between a parent-teen mobile phone safety technology's users and the emergency responders.

Be accommodating to device resources. In addition to all the above lessons and goals, we observe that a parent-teen mobile phone safety application must also be sensitive to the resource constraints on the mobile phones: power, latency, computational power, and so on. Since these are standard challenges for mobile phone applications, we do not describe these challenges further here.

Based on the above lessons and associated challenges, we now present several technical recommendations for the design of future parent-teen mobile phone safety technologies. These recommendations are in addition to our recommended use of notifications, awareness, and control mentioned above.

Separate encryption pathways for different data. Because not all data are created equal and neither are the recipients, we envision significant utility coming from separate encryption pathways for different data. For example, photos of the teens may be decryptable just by the police, while coarse location information may be decryptable by the parents as well. This technique may help with collecting sensitive information – photos with possible indirect stakeholders may only be accessible to emergency responders, or only be accessible when emergency responders and parents collaborate (e.g., when a teen is determined to be missing); we describe this technique further below. This separation may also help in not intensifying abusive parent-teen relationships by making some of the collected information unavailable to parents.

Multi-party decryption. For a stronger level of protection, some data should only be decryptable through the collaboration of multiple parties (e.g., police, parents, and telephone service provider) – for example, when multiple parties must work together during a teen's disappearance. One approach for achieving this in a simple iterative manner is to encrypt with one key, then another (each of which belong to a different party). A risk with this approach is that the last party to decrypt could be malicious and not reveal the resulting decrypted data to the other participating parties. It is also possible to use more sophisticated multi-party decryption techniques, e.g., [25].

State transitions with phone-detected emergencies. When the phone itself detects an emergency, it should make more information available. For example, if the phone detects that the teen has been in a car crash and is no longer responsive to prompts, it might no longer encrypt the teen's location information as it alerts the authorities or the application's service provider. To amplify privacy, and recalling our argument for separate pathways for different data, the application's service provider should only be able to see the information necessary to determine whether a real emergency response is needed; the remaining information could be decryptable only by the emergency responders.

State transition if phone destroyed in emergencies. Some emergencies may be difficult to detect reliably solely on the phone because the phone itself may become inoperable during the emergency (e.g., during a car crash). Ignoring privacy, a natural approach in would be to have the service provider constantly monitor the teen's phone data, detect anomalies, and then trigger responses. However, for privacy, teens and parents may only want to expose that information to emergency responders, and only when there really is an emergency – and explicitly not to the provider of the parent-teen mobile phone safety service. Hence, full information about the teen's context may only be decryptable by the emergency responders, or by the emergency responders and the service provider when cooperating using multi-party decryption. The service provider by itself cannot decrypt. The conundrum is, therefore, how to allow the service provider to detect an emergency situation.

An approach for overcoming this challenge may be for the phone to register (low-information) events with the service provider that, if not canceled, would cause the service provider to take emergency action and forward full-context encrypted information to emergency responders. For example, if the phone detects that it is traveling above 90 miles per hour, it may instruct the server to contact the emergency responders and forward encrypted location information if the server ceases to receive updates from the phone. As another example, a user could press an "I feel unsafe" button on his or her phone, which periodically sends keep-alive messages and video traces (that only emergency responders can decrypt) to the server while depressed. If the keep-alives ever stop, but the user does not perform the explicit "cancel I feel unsafe" procedure within a reasonable time, then (in the worst case) the phone might have been taken from the teen or destroyed, and the third-party service will notify emergency responders. To minimize the risk of false positives (e.g., when the phone enters a long tunnel), the emergency responders could conduct another layer of filtering after decrypting the data.

Regular information destruction. Information should be deleted once it is no longer needed, and special processes should be in place to handle information destruction. Recent directions in self-destructing data, such as Vanish [17] and on-going research, could be used to encapsulate data so that the data cannot be accessed after a certain period (e.g., first apply something like Vanish, and then encrypt). Furthermore, when data is accessed for emergency purposes, the system should ensure that it cannot be accessed later, after the emergency is resolved. While this may require some trust in the party accessing the information (i.e., that it will destroy the data after use), the data should not be available to other parties in the future (e.g., other branches of the government).

Panic passwords and covert communications to counter coercive environments. Systems should provide covert ways of communicating with parents and other parties. For example, certain "spam" text messages may actually be secret messages from parents. Alternatively, the teen could use panic password [7] techniques to indicate an alarm. For example, entering the regular PIN will unlock a phone, while entering another, special PIN could send a pre-specified message to the parents; the message could be "please call me and ask to pick me up; I want to leave." Similarly, the "cancel I feel unsafe" procedure mentioned above in the context of destroyed phones could have two "cancel" actions or PINs: one PIN that really cancels the "I feel unsafe" action and another PIN that *appears* to cancel that action but in actuality sends an urgent distress message to the service provider.

6. CONTRIBUTIONS AND FUTURE WORK

Our contributions are at two levels. One level concerns a specific set of "parenting technologies" and tools for mobile personal safety. We use theory and methods of Value Sensitive Design to systematically analyze the different stakeholders, both direct and indirect, who are affected by these systems, as well as the values at stake, such as privacy, safety, trust, and maturation. We report on the results of in-depth semi-structured interviews with 18 participants (9 teens and 9 parents) regarding their views and values on such technologies. Analyzing these interviews shows significant differences with respect to different kinds of information (e.g., mood vs. location), situations (e.g., emergency vs. non-emergency), and the acceptability of solutions when notification may or may not be present. Based on these results, we then identify key technical challenges and architectural hooks to help support positive values, such as privacy and trust, and avoid some of the potential negative impacts of such systems.

At a broader level, we use this work to demonstrate how to apply Value Sensitive Design effectively to complex security problems, particularly those for which there is no clear-cut set of assets, risks, and affected parties. We use and extend several techniques from Value Sensitive Design, including developing value scenarios, and assessing alternate approaches using the values dams and flows method. A methodological contribution is a new method for studying impacts on direct vs. indirect stakeholders, in which the same study participant engages with a technical system first from perspective of a direct stakeholder and then from that of an indirect one. We then show how these analyses can be used to develop technical strategies for designing secure and private mobile phone safety technologies, including empirically informed decisions regarding what data to collect, when to notify, and whom to notify.

We hope that the work reported here will thus provide a robust foundation for future work on mobile phone safety technologies, as well as serving as a prototypical example of using Value Sensitive Design to explicate the underlying human values in complex security domains.

7. ACKNOWLEDGMENTS

Many thanks to all teens and parents who participated in our study and to Nell Carden Grey for her help in writing the value scenarios. This research was supported in part by NSF Award CNS-0905384.

8. REFERENCES

[1] PC Tattletale internet monitoring software & parental control software, 2009. http://www.pctattletale.com/.

[2] B. F. Batya, P. H. Kahn Jr., J. Hagman, R. L. Severson, and B. Gill. The watcher and the watched: social judgments about privacy in a public place. *Human Computer Interaction*, 21(2):235–272, 2006.

[3] A. Beresford and F. Stajano. Location privacy in pervasive computing. In *IEEE Pervasive Computing*, 2003.

[4] D. Boyd and J. Heer. Profiles as conversation: Networked identity performance on Friendster. In *HICSS-39*, January 2006.

[5] BrickHouseSecurity.com. Cell phone spy, 2009. http://brickhousesecurity.com/cellphone-spy-simcardreader.html.

[6] BrickHouseSecurity.com. BrickHouse child locator with wander alerts, 2010. http://www.brickhousesecurity.com/child-locator.html.

[7] J. Clark and U. Hengartner. Panic passwords: authenticating under duress. In *HOTSEC'08: Proceedings of the 3rd conference on Hot topics in security*, pages 1–6, Berkeley, CA, USA, 2008. USENIX Association.

[8] J. Davis, P. Lin, A. Borning, B. Friedman, P. H. Kahn Jr., and P. A. Waddell. Simulations for urban planning: Designing for human values. *Computer*, 39:66–72, 2006.

[9] J. DeFao. Parents turn to tech toys to track teens, 2006. http://bit.ly/trackteens.

[10] T. Denning, A. Borning, B. Friedman, B. Gill, T. Kohno, and W. H. Maisel. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proc. CHI 2010*, pages 917–926. ACM Press, 2010.

[11] DriveCam, Inc. Driver safety and fleet safety vehicle safety | DriveCam driver risk management, 2009. http://www.drivecam.com.

[12] Y. Duan and J. Canny. Protecting user data in ubiquitous computing environments: Towards trustworthy environments. In *Privacy Enhancing Technologies: Proc. 4th International Workshop (PET 2004)*. Springer, 2004.

[13] J. L. Fleiss, B. Levin, and M. C. Paik. *Statistical methods for rates and proportions*. John Wiley & Sons, third edition, 2003.

[14] B. Friedman, P. H. Kahn Jr., and A. Borning. Value Sensitive Design and information systems: Three case studies. In *Human-Computer Interaction and Management Information Systems: Foundations*. M.E. Sharpe, Armonk, NY, 2006.

[15] B. Friedman, P. Lin, and J. K. Miller. Informed consent by design. In *Designing Secure Systems That People Can Use*, pages 495–521. O'Reilly and Associates, 2005.

[16] B. Friedman, I. E. Smith, P. H. Kahn Jr., S. Consolvo, and J. Selawski. Development of a privacy addendum for open source licenses: Value Sensitive Design in industry. In *Ubicomp*, pages 194–211, 2006.

[17] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy. Vanish: Increasing data privacy with self-destructing data. In *Proc. of the 18th USENIX Security Symposium*, 2009.

[18] M. Group Media. Is That an Interesting Conversation?, 2009. http://groupmedia.media.mit.edu/interest.php.

[19] G. Iachello, I. Smith, S. Consolvo, M. Chen, and G. Abowd. Developing privacy guidelines for social location disclosure applications and services. In *Symposium on Usable Privacy and Security*, 2005.

[20] A. Jacobs and G. Abowd. A framework for comparing perspectives on privacy and pervasive technologies. In *IEEE Pervasive Computing*, volume 2, 2003.

[21] X. Jiang, J. I. Hong, and J. A. Landay. Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. In *UbiComp*, 2002.

[22] P. H. Kahn, H. Ishiguro, B. Friedman, and T. K. What is a human? Toward psychological benchmarks in the field of human-robot interaction. In *Proceedings of the 15th International Symposium on Robot and Human Interactive Communication (RO-MAN '06)*, pages 364–371. IEEE, 2006.

[23] A. LaMarca, Y. Chawathe, S. Consolvo, J. Hightower, I. Smith, J. Scott, T. Sohn, J. Howard, J. Hughes, F. Potter, J. Tabert, P. Powledge, G. Borriello, and B. Schilit. Place Lab: Device positioning using radio beacons in the wild. In *Pervasive Computing*, 2005.

[24] J. Landis and G. Koch. *The Measurement of Observer Agreement for Categorical Data*. Biometrics, 33, 1977.

[25] P. MacKenzie. An efficient two-party public key cryptosystem secure against adaptive chosen ciphertext attack. In *PKC*, 2003.

[26] N. Marmasse and C. Schmandt. Safe & sound: a wireless leash. In *Ext. Abstracts CHI 2003*, pages 726–727. ACM Press, 2003.

[27] J. K. Miller, B. Friedman, and G. Jancke. Value tensions in design: the value sensitive design, development, and appropriation of a corporation's groupware system. In *GROUP*, pages 281–290, 2007.

[28] L. I. Millett, B. Friedman, and E. W. Felten. Cookies and web browser design: toward realizing informed consent online. In *Proc. CHI 2001*, pages 46–52. ACM Press, 2001.

[29] E. Miluzzo, N. D. Lane, S. B. Eisenman, and A. T. Campbell. CenceMe – injecting sensing presence into social networking applications. www.cs.dartmouth.edu/~campbell/cenceme.pdf.

[30] Mobile Teen GPS. GPS vehicle tracking for teen drivers, 2009. http://www.mobileteengps.com/.

[31] Monitoring Software Reviews. Parental control software & internet monitoring software reviews, 2009. http://www.monitoringsoftwarereviews.org/.

[32] My Mobile Witness, Inc. My Mobile Witness(sm), 2008. http://www.mymobilewitness.com.

[33] G. Myles, A. Friday, and N. Davies. Preserving privacy in environments with location-based applications. In *IEEE Pervasive Computing*, 2003.

[34] L. P. Nathan, P. V. Klasnja, and B. Friedman. Value scenarios: a technique for envisioning systemic effects of new technologies. In *Ext. Abstracts CHI 2007*, pages 2585–2590. ACM Press, 2007.

[35] NaVee Technologies, LLC. FreeFamilyWatch, 2008. http://www.freefamilywatch.com.

[36] L. Skenazy. *Free Range Kids*. Jossey-Bass, 2009.

[37] WebWatcher. Monitor computer use with remote computer monitoring software, 2009. http://www.webwatchernow.com.

[38] C. White. Bladerunner GPS jacket locates kids, replicants, 2009. http://tinyurl.com/GPSjacket.

[39] S. Yang, Q. Li, X. Wang, Y. Li, and R. Huang. Analysis on the prospects of parent-adolescent communication served by mobile technology. In *WMUTE '08: Proceedings of the Fifth IEEE International Conference on Wireless, Mobile, and Ubiquitous Technology in Education*, pages 213–215, Washington, DC, USA, 2008. IEEE Computer Society.

APPENDIX

A. VALUE DEFINITIONS

The following are the definitions for values that our participants were asked to consider. The definitions are given from the teen point of view; for parents the definitions were adjusted appropriately.

- Safety – Ability to be protected from any type of harm (physical, social, emotional, etc.)
- Trust (you) – Ability to be trusted by your parent (have your parent trust you).
- Informed Consent – Ability to understand what you're agreeing to. Ability to participate or withdraw from an activity at your discretion.
- Trust (him/her) – Ability to trust your parent. By trust, we mean to have confidence in, be able to rely on, and make yourself vulnerable (emotionally or mentally).
- Ability to Make Mistakes and Take Responsibility – Ability to make mistakes and take responsibility for your actions.
- Autonomy – Ability to be in charge of your own actions and make your own decisions.
- False Sense of Security – Ability to know if you are safe or not and to be able to recognize when a situation has the potential for danger.
- Freedom From Misrepresentation – History of what you have done is preserved accurately. Others can neither claim you did something if you didn't nor claim you didn't do something you actually did.
- Groundless Fear – Ability to not be scared when there is nothing to be scared of.
- Privacy – Ability to control where, how and to whom your information is released. Ability to seclude yourself or some information about you from others if you so choose.
- False Alarms – Ability to not have other people (emergency responders, friends, family) notified that you are in an emergency situation when you're not.
- Spontaneity – Ability to do as you please as a result of an on-the-spot decision – without prior planning or preparation.
- Property – The feeling that an object belongs to you and that you have control over what happens to it and what it does.
- Reliance on Technology – Ability to avoid becoming reliant on new technologies.

Value	**% of parents who "care a lot" about the value**	**% of teens who "care a lot" about the value**
Safety	100	88
Trust (you)	100	88
Informed Consent	100	75
Trust (him/her)	100	75
Ability to Make Mistakes and Take Responsibility	100	63
Autonomy	89	88
False Sense of Security	89*	25*
Freedom From Misrepresentation	78	50
Groundless Fear	78	50
Privacy	67	50
False Alarms	44	50
Spontaneity	44	63
Property	22	25
Reliance on Technology	22	25

Table 3: Percentage of parents and percentage of teens who "care a lot" about these values. (Parents: N = 9; Teens: N = 8; Note: an '*' indicates a statistically significant difference.)