1 Introduction
Technology is the stuff of dreams. It’s the answer that turns what is into what ought to be. It’s the hope for Massive Change for the betterment of all mankind (Mau et al., 2004). It’s the iPhone that keeps us always “connected.” It’s even the frivolous toy one might find on a gadgets website like ThinkGeek (www.thinkgeek.com). The problem with new technology is that there is more often than not a chasm between who gets to invent it and who gets to (or has to) use it (Harding, 1993). Furthermore, technology is born (Bucciarelli, 1994) (or suppressed (Latour & Porter, 1996)) on the account of politics and lives in support of political agendas (Winner, 1980). The sum of these facts not surprisingly results in a culture of technology for the sake of technology (Henninger, 1991). Thus, towards developing more democratic and appropriate technologies, we must first look at what new technologies mean to their users, and how they reshape users’ day-to-day activities.

We’ve all heard of the “paperless office” (Week, 1975), and subsequently of the “myth” of the paperless office (Sellen & Harper, 2003). But, the swing towards digital media has continued as new technological innovations make possible digital music management, streaming video, eBook reading (e.g. iTunes, NetFlix, Amazon’s Kindle, respectively), and more. The situation becomes increasingly complex as we add in the factors of sensitive information and privacy. These issues have recently come to the forefront with the invention of personal information management (PIM), and is crystallized in at least one recent movement to the digital in the area of medical health records (Veen, 2008). From this and similar conversions from physical to digital information management emerges the need to keep private information secure. But, this task of maintaining the appropriate degree of information accessibility amongst parties is not simply a matter of technological security, but also one of social usability; the social, contextual circumstances (not solely the mechanical robustness) of the technology greatly influence the security of the information. Furthermore, at least two important pieces of information that might prove instrumental to the design of usable and secure information managements systems are still mostly unexplored: the ways in which information is physically managed already and social environments in which technological solutions might be deployed.

To begin to fill in these gaps, we have taken an approach that aims to work from existing user needs as opposed to working from technological possibilities: to study the existing, socially-mediated practices of information management in real work contexts. Through the lens of an ethnographically-informed study of four childcare centers, we offer reports of socially-rich information practices that have direct bearing on information security. We find that the dynamic, unpredictable nature of day-to-day childcare affairs renders improvisation a requirement. Ideal information practices are thus foiled by unexpected events and the resulting situated security measures hinge on various forms of politically-mediated gatekeeping. Finally, we discuss the dynamic between information provider and information manager—the parent-
director relationship—and discover various asymmetries of information awareness, access, and control. From these observed insights, we draw three important issues to the attention of usable security: the difference between sensibility (of human activity) and regularity (or program output), between digital and physical security sense, and between centralized and decentralized information management. The descriptions and particular findings included here will provide a platform for comparison to digital repositories and for discussion about how we may improve upon the current situation. We begin in the next section by introducing usable security and the electronic personal health records.

2 Background

Computer Science has long history of finding technical security mechanisms to protect sensitive information, but it wasn’t until recently that the issue of usable security began to surface (Week, 1975; Whitten & Tygar, 1999). The important revelation was that the technology could not predetermine how users would appropriate it; hence, the robustness of security mechanisms were only part—the more predictable part—of a holistic security system. When the human factor is left out of the security equation, the security of the technical system is susceptible to compromise through human appropriation.

Personal information management (PIM) is one field that that concerns itself with the many personal information artifacts that we create daily in our encounters with the digital world. Desktop, laptop, PDA, cell phone technologies all have applications that allow users to create and share information. PIM inspects how information is created and accessed by individuals with such devices and how this task can be facilitated through appropriate interfaces. Due to the diverse architectures of these platforms, the diverse information (and often personal) that is stored on them, and the diverse ways in which users appropriate them, information management is increasingly difficult. Furthermore, various parties are involved in the information maintenance and ownership; not all personal information about an individual is created by that individual. For example, organizations store information about customers and employees. Digitization of information in all areas of our lives is posing new questions related to ownership, accessibility, and security of information that is personal in nature but gained or acquired by other parties like health care professionals. (Jones, 2006)

More and more people are archiving their personal digital information. Information is not only stored in a local machine but also accessible on or offline. Not only the architecture is distributed but the application across which the information is stored varies vastly (Marshall et al., 2006). Their research was geared towards digital artifacts created or collected by the people like photos, video recordings, and documents. Generally inaccessible personal information residing in an organization—health records, for example—was out of the scope of the research. Civan et al. conducted a study on personal health information management (Andrea Civan 2006). Findings in their study indicate that individuals want access and control over their health information. While they want to share their information with their clinicians they also wanted to dictate the amount of information that would be shared. Perhaps the most interesting of all the findings was that participants identifying the trade-off between usability and security. They wanted a system that is easy to use yet keeps the information secure.

With the recent developments of ubiquitous and tangible computing, context has taken center stage in the study of usable security (Schilit et al., 1994). Many of the initial developments of this effort defined context in the spirit of modernism—encodeable data that is both predefined and prescriptive of user behavior. This notion has since been balanced with a more post-modernist interpretation that recognizes context as richly-variable and socially-constructed in situ (Dourish, 2004). The latter implies ethnographic methods for probing the ground-level social construction processes that directly speak to how we might create usable and secure systems. The work presented here is grounded in the latter approach.
One of the earliest works in this vein was that of Harrison & Dourish (Harrison & Dourish, 1996), in which privacy was identified as a social construct as opposed to a set of “psychological primitives.” Although technology (such as walls, doors, or permission lists) does play a role in privacy, without consideration of human constructions, it cannot adequately describe the notion of privacy. This paper also comments on the relationship between physical and digital conceptions of space; different electronic media have different spatial qualities, which in turn affect the patterns of use, adoption and adaptation of media environments. On the topic of both privacy (a human distinction) and security (a technological distinction), Dourish and Anderson (Dourish & Anderson, 2006) recapitulate that these must not be considered simply matters defined by rational economic decision-making (as suggested by many researchers, including (Herley, 2009)); they must be observed as social, cultural constructions that are in constant conversation with themselves. In a paper with similar goals as this, Dourish et al. (Dourish et al., 2004) use qualitative investigations to identify security practices in a workplace context. Several of their findings have been independently identified in similar forms in this work and extended. These include the use of “cryptic email” messages for security, the manipulation physical office space to construct public and private space, and the delegation of security to other parties.

One particularly relevant new development with regard to privacy and security in digital information management is the new interest in digitizing files into personal health records (PHR’s) (Veen, 2008). PHR’s are the new vision (as being promoted by Google Health and Microsoft’s HealthVault systems) for digital versions of patients’ medical file folder contents. PHR’s are stored on the service provider’s servers in compliance with the privacy and security standards established by HIPAA (Veen, 2008). PHR’s put patients in control of their own health records, as opposed to the current system which leaves the matter of ownership ambiguous and hence subject to legal interpretation. This new infrastructure does not come without a new set of security and privacy risks—the threat of malicious digital attacks, ease of data copying and manipulation in data mining algorithms, etc. And, there is also a sense of opportunity for applications that will encourage healthier living and patient empowerment. At the most basic level, PHR’s represent the movement of potentially sensitive data to centralized, digital repositories and thus are one application for which the data presented here will be relevant.

3 Approach
This research approaches the question of childcare information management from an ethnographic methods perspective. Ethnographic methods are particularly attuned to finding “the strange in the familiar” (Marvasti, 2004). This is precisely our goal: to identify the nuanced information security activities that may be altered or lost when moving to digital repositories. For computer scientists, this often means looking past the abstract, intuited plans we (and even the participants themselves (Bucciarelli, 1994)) prefabricate to the situational, lived practices we observe. Through interviews and observations we can learn what information practices mean to the participants and see how they are carried out. The ethnographic approach in turn impacts everything “from forming a research question, to data collection, and to writing and reporting the findings” (Marvasti, 2004). Table 1 gives an overview of the steps that we followed in our study. This study was part of a larger, ongoing research project. We started with a data review session in which we read earlier transcripts and reports. We then constructed interview protocols, conducted the interviews and observations, transcribed our data, and lastly coded them. Section 3.1 and 3.2 provide more details on each of these steps.

3.1 Data Collection
Four childcare centers participated in this research, each group member working with two of them. Table 2 gives some general information about the participating centers and directors. One participant represented each childcare and held the position of either director or assistant director of her facility. These directors were drawn from a previous study of childcare information management (in which 12 directors were interviewed). Their participant IDs carry over from the initial study: P1, P3, P4, and P6.
For one of the centers, in the absence of the director, the researcher shadowed the program manager and office assistant. The director position generally implies charge of managing the daily happenings at the childcare and keeping the center compliant within industry regulations (although we will see that the duties of the director extend far beyond their official job description). Independently, both researchers conducted an hour-long interview with each participant, followed by three separate observations sessions that lasted from 2-3 hours each.

Interview sessions were held as the first point of contact with participants. This was done in order to establish a more comfortable relationship with the director before less structured (and hence potentially...
more socially awkward) observation periods. Because this study followed from a previous study, these participants had already been interviewed months earlier about their information practices; transcripts from these initial interviews (carried out by another researcher) were used to formulate an interview protocol to be shared by both researchers. The interviews were semi-structured, meaning that we had prepared interview questions in advance, but we followed interesting leads with impromptu questions as they arose. Interviews were audio recorded and notes were taken on paper throughout. During one of the four interviews, the audio malfunctioned and was lost; hand-written notes were the basis of analysis for this interview.

Observations began either on the day of the interview or at a later date. These sessions lasted 2-3 hours each, and 3 observations were carried out for each director. Participants were told that we would like to “shadow” them through part of their work day in order to see how they work and get a feel for the work environment. As “shadowing” implies, the researcher followed the director as she moved throughout her day, though this was not always the case. However, the researchers decided that it was best to be a partial-participant—to engage with the directors for some casual as well as some work-related discussion. Sometimes this meant laughing together, others it meant asking her for an explanation of her activities, and for others it meant that she offered unprovoked information about her activities. Field jottings and time stamps were recorded throughout observations sessions, roughly 8 pages of field notes per hour. Audio recordings were also taken by one researcher via a visible audio recorder around her neck. The other researcher used the audio recorder once but then discontinued use because she sensed that participants were nervous around the device. Pictures, if allowed, and artifacts (forms, etc.) were taken from within the childcare to further document the experience. In addition to interview and observation data, the researchers kept track of contacts made with participants: phone calls, interviews, and observations. Each contact was listed with a date, an even description, and a description of any critical incidents that might be important to share.

In preparation for the observation, the researchers agreed upon some loose themes (e.g. ownership, communication breakdowns, tangibility of information, physical gatekeeper in front of the file cabinet, and duplication of physical files to digital) to explore; these were identified from the initial base of 12 interviews from the previous research project. The researchers, however, agreed to keep an open mind in the field and to begin by writing down all aspects of the experience as possible. As previously-mentioned the observers became pseudo-participants in the field—asking questions and interacting casually with the directors and other passersby.

<table>
<thead>
<tr>
<th></th>
<th>P1</th>
<th>P3</th>
<th>P4</th>
<th>P6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours of operation</td>
<td>7:15 am – 4:45 pm</td>
<td>6 am – 6 pm</td>
<td>7:30 am – 5:30 pm</td>
<td>7 am – 5:45 pm</td>
</tr>
<tr>
<td>Enrollment Size</td>
<td>200</td>
<td>200</td>
<td>43</td>
<td>100</td>
</tr>
<tr>
<td>Age</td>
<td>6 wk – 12 yr</td>
<td>6 wk – 12 yr</td>
<td>15 mo – 5 yr</td>
<td>6 wk – 12 yr</td>
</tr>
<tr>
<td>Title</td>
<td>Director</td>
<td>Director</td>
<td>Director</td>
<td>Director</td>
</tr>
<tr>
<td>Gender (director)</td>
<td>Female</td>
<td>Female</td>
<td>Female</td>
<td>Female</td>
</tr>
<tr>
<td>Staff Size</td>
<td>30</td>
<td>45</td>
<td>15</td>
<td>22</td>
</tr>
<tr>
<td>School Van</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Number of observations</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Hours of observation</td>
<td>9</td>
<td>9</td>
<td>5</td>
<td>9</td>
</tr>
</tbody>
</table>

Table 2: overview of basic childcare and director information
The data collected in the field was transcribed by each researcher. Audio recordings of interviews were transcribed (~15 pages each), and much of the dialogue from observation recordings was transcribed, as well. Field jottings were turned into field notes with the synthesis of pictures, artifacts, hand-drawn diagrams, and key dialogue snippets (~35 pages each for audio-based observations, ~10 pages each for the rest).

3.2 Analysis

The researchers took a grounded theory approach to analysis, with iterative coding, cluster diagramming, and memo writing. Coding and data analysis took place both independently and jointly amongst the researchers. Coding refers to the process of “categorizing segments of data with a short name that simultaneously summarizes and accounts for each piece of data.” In the field, during the process of observation, initial coding ideas were sometimes jotted down for later attention. For example, the codes from one researcher on the first day of her observation were: “constant phone/office interruption,” “duplication of information,” “good communication abilities,” “the door is a place of much conversation,” and “small world community.” These continued throughout the observations. (Bryant & Charmaz, 2007)

A new variety of coding began as the researchers became more immersed in the data and ideas came outside of observations; higher-level coding ideas coupled with paragraph-length descriptions were typed in emails and passed around to the group for comments (e.g. “childcare activities as improvisational,” “duplication of duty/information,” “using visible accessibility to manage security,” “reactive policy development,” and so on). A dozen or so of these emails circulated, including possible meta-codes and theories that we might link our work to (e.g. “duplication of information as a way of achieving robust network,” “accessing unauthorized information in a physical system is less morally damaging than hacking on a virtual system,” and “people understand security tradeoffs better in physical environments because the mechanisms are more visible and intuitively understood”).

Finally, a code-based cluster diagram was constructed to identify common themes and relationships amongst the emerging codes of both researchers. Several memos—thorough articulations of codes and their connections to one another—were written to describe the three large groupings of codes that were developed in the cluster diagram. Memos thus grouped several codes, describing and giving examples of each as well as providing a discussion of relationships to other codes. This development culminated in a 5-hour meeting during which we placed all postulated codes on the table and came to dialectical consensus on a subset of 32 codes. These methods constitute our grounded theory approach to analysis. (Bryant & Charmaz, 2007)

4 Data

The childcare is a place apart from any other; from dawn to late afternoon its halls are filled with the curious questions, wailing shrieks, and pattering feet of children from up to 200 families. All are in the care of just a few dozen teachers—mostly young to middle-aged women—and under the charge of one or two very busy directors. Take, for example, that in the first five minutes of observation at P1’s facility, P1 was interrupted from her seemingly primary paperwork task no less than 7 times by 7 different people with 7 different needs. And, while P1 sometimes leaves home almost “crying because [she] can’t get [her] work done,” and P4’s desk is swimming in paperwork piled high from the last time she went out of town, the directors seem to really love their job as far as it pertains to all the “little lives” that they watch over every day. In fact, childcare as a job to the directors is at least partially about fulfilling the sacred duty of keeping children safe, teaching them—essentially “raising them.” On the other hand, childcare as a job cannot escape its necessary charge as a business that needs to stay licensed, maintain customers, and make a profit. These two salient and, at times, dualistic identities are important pieces of the driving forces behind childcare workers’ mentalities, culture, and thus information management.
The ‘childcare-as-sacred-practice’ hat identifies the children’s well-being as a matter of utmost importance, one that seems to go beyond the responsibility of business and into intrinsic duty. In defense of a strict security measure, P1 says in a romantic tone, “well, it’s lots of little lives” that hang in the balance. The licensor also shows this leaning when she explains that it’s not only a matter of business that makes it necessary to be diligent about which students are accounted for, but it’s also a matter of “try[ing] to protect the lives that you serve.” And, when P4 discusses how mistakes are usually confined to minor miscommunication issues she also alludes to the sacred nature of childcare: “there are—you know, it's hard to communicate in this business just because we're always so busy, but we do it where it counts. I mean, it counts everywh—you know to protect the children.” And, she does this again with regard to the same topic: “we sort of acknowledge that we're here to do what's best for these children.” The other hat—‘childcare-as-business’—comes on and off in fluid exchange with the sacred duty of child rearing.

P1 identifies the need to worry about litigation regarding negligence: “but, what's scarier, the parent losing the child, or the teacher losing the child? I was like, you can sue us... you can be mad at yourself, but you can sue us, and that's just not a risk we're willing to take.” The licensing agent agreed that “no matter what you do sometimes, it's never enough because you just can't prevent everything from happening, but at least you can protect yourself.” Business surfaces again when P1 considers the cost of switching to paper towels that would be more appropriate for the classroom activities. And, directors indicate that they are fortunate when the licensing agent does not publicly write them up for their violations. Here, we see the sacred practice of childcare giving way to a more basic need to keep the business safe. These two hats form a basis for directors’ modes of thought and surface in the details of everything we will see them do in the following sections.

But, before we dive deeper into the world of the childcare, let us first clarify our distinction (or lack thereof) between the general practices and the information security practices that we witnessed. Like (Adams & Blandford, 2005), we consider the security and privacy of information practices to be inextricably linked to the attitudes, perceptions, and roles that individuals exhibit within the workplace. Hence, we will draw not only from explicit security-related incidents (e.g. a door found unlocked), but also from incidents that more broadly display attitudes and practices that may impact security (e.g. a child’s car seat found unbuckled exhibits policy breakdown). From this standpoint, information security practices are a sub-practice of the childcare, and as such, it works within the overall framework of childcare order; what we learn from one is applicable to the other.

The next four sections are dedicated to data collected in the field. Section 4.1 identifies some of the basic information gathered on different time scales and then describes some of the policies that govern management of that information. Sections 4.2, 4.3, and 4.4 present three main codes identified in analysis and selected sub-codes that have bearing on usable security in digital information management.

### 4.1 Data collection and regulatory policies

Childcare centers gather and maintain data not only about the children that they host, but also about the parents and their own employees. Various data concerning these parties is collected at different frequencies throughout the year. Below we have listed some of the most common information and collection procedures based on their frequency of collection.

#### 4.1.1 Yearly

Some information is required only once. For example, parents have to provide their information (name, address, phone number, work address, work phone, SSN, etc.) along with their child’s information (anything from name and birth date, to allergies and immunization records, to food preferences and temperament) at the time of initial enrollment. P3 mentioned that the parents also have to update all the information yearly as a requirement for the licensing of the center. P3 says that many parents are reluctant to fill out the paperwork from scratch and sometimes they write “same” in the fields.
On a different note, P6 mentioned that they combine all the accident/incident reports of a year and create an annual accident/incident report. They keep this file for licensing and shred the original reports. This year end accident report is used to see if any class needs to change anything for recurring accidents.

4.1.2 Semi-Annually
The centers also get information semi-annually. P3 mentioned that the licensing inspector usually visits the center twice during a year. During the visit, the inspector goes through the classrooms to make sure the state requirements are met. They also look at the files of children for up-to-date information. For a provisionally-licensed center—one that has just opened—there is an initial inspection immediately before the center opens and the first six months is marked by two unannounced inspections. When repeated violations are identified, inspections may become monthly.

4.1.3 Monthly
Some of the families in the centers get support from the Department of Social Services. For this the centers have to provide a monthly attendance list of the children to DSS. Beside this, some centers have their own tasks that they do monthly. For example, P3 does a precautionary monthly check on the classes to see if they meet the licensing requirement.

P3 creates a center-wide newsletter at the end of each month that lists activities for the coming month. Teachers from each class create a separate newsletter that goes to the parent, which lists class activities of the next month. They also include reminders, such as bringing weather-appropriate garments for upcoming cold weather. Aside from the newsletter, the teachers also provide a supply list to the office, things that will be required for doing class activities. They are also supposed to provide an AM and PM activity list for the class.

P4 and P6 create a meal plan monthly and puts a copy of it in the parent notice board. According to P6, a lot of parents take this diet plans and she has to make more copies 2-3 times in a month. She said that this information is helpful for parents because some of the children may have dietary preferences or restrictions and the diet plan helps the parents to be prepared for these scenarios.

4.1.4 Bi-weekly
The two most prominent bi-weekly activities seen in the centers were payroll and the tuition. P6 mentions that she does tuition and payroll twice a month. For payroll, she totals the hours for each employee. If there are some missing hours she looks at the leave request file to make sure that those hours are not from an already granted leave. Based on this information, she creates the payroll. For tuition, she writes down the receipts and places some of them in a receipt box for parent pick-up upon request (the parents put a paper clip on their tuition envelope indicating that they want a receipt). Then she enters the information in QuickBook, an accounting software because “it’s nice to have another copy.”

4.1.5 Weekly
Some of the centers follow their own weekly schedule. At the end of each week, P3 prints a set of clean forms for collecting attendance, expected van pick-ups and drop-offs, and meals eaten by children throughout the day for each classroom. She also does a weekly check on the time card entries listed by the employees to make sure the times they come in and go are correctly entered into the system. The employees use a keypad, which is connected to a computer, to enter the time they come and leave. P3 said that sometimes they don’t clock in properly and fail to tell her. This can create inaccuracies in their payroll. She doesn’t wait until the last moment and checks this information weekly instead of biweekly when checks are cut.
P6 creates the employee schedules weekly. Each week the employees are supposed to look at their mailboxes to see their schedule for next week. Although the schedules are made and posted daily in the staff notice board, during the observation session the researcher noticed a lot of schedule change requests.

4.1.6 Daily
The attendance log of children is updated daily in almost all the centers. In P3, the teachers sign in and out the children while in P6 parents are the one who sign in the attendance sheet. The teachers also log their hours in the center in some form. Some centers use timecards (P6) and some use an electronic system (P3).

P3 does a ratio count frequently throughout the day. During ratio count, the director/office assistant /program director calls each class and asks for the number of teachers and students in the class. They make sure that there is 1 teacher for every 4 children to stay in compliance with licensing requirements; this is called “maintaining ratio.” Usually it is the program director in that center who does the ratio count in the morning, every half an hour until 9 am. The evening hour ratio count is done every half an hour in the evening by the office assistant.

Some of the centers provide rides for children to and from schools. They use forms in the vans to log information regarding the van rides on a daily basis. P3’s van form lists children’s names and teachers mark who was absent and present that day so that they can know which children to expect to pick up. P6 on the other hand only logs information related to the van, for example – the reason for using the van, date, time and its mileage.

Some of the centers provide meals and they document the children’s eating information in different ways. For younger children they usually list the amount of food they had. For older children they only note if the child ate his/her meal. Almost all the centers have a teachers log for logging suspicious events relating the children. The teachers look for any indication – physical signs or verbal account of possible abuse. They also look for symptoms of disease. These logs are secret and the writings are not made open to anyone other than the director unless an official complaint is filed.

Children of most centers take home a report that indicates how their days went in the center. Some classes in P3 have a report with three faces: smiley, normal and frown. P6 mentioned that for younger children, their daily activity is posted in the message board and the parents can pick them up from the board. This form has information like how many times the diaper was changed, condition of diaper, time of meals and the amount etc. For older children, they take home a form containing some adjectives that describe their days. The forms are placed in the cubbyholes for the parents to pick-up. According to P6, some parents are very serious about these forms while others do not take them seriously and only glance over it.

In many centers, employee schedules are posted daily. Although P6 creates the weekly schedule, the daily schedules are posted in the staff board everyday. Similarly, P3 creates a daily schedule for the teachers and staff of the center. On top of that, they constantly redirect substitutes or volunteers on classes when necessary throughout the day.

4.1.7 Update Information
Centers make sure that they have up-to-date immunization history of each child. This is a licensing requirement. P6 mentioned that if parents don’t immunize their children, the center have a form that says “choose not to immunize” which must be signed by the parents. The centers are also required to have up-to-date contact information of the parents. P3 mentioned that parents are supposed to notify the center when they change their address.
4.1.8 Periodic
The centers follow different communication policies for parents. For example, P6’s center holds a parent teacher meeting at regular intervals. She said that this meeting happens on a periodic basis throughout the year, roughly every other month, more often if needed. The message boards on the doors of the classrooms are another way of communicating with the parents. For example, the whiteboard in the door may have a message reminding the parent of the coming field trip.

Accident and incident reports are created when, for instance, one child bites another. The form requires 3 signatures: one from the class teacher, one from the center director and the last one is from the parent. Accident reports are done for the injured child and the parents get a copy of this. The incident report, which is not given to anyone, is filled up for the child who caused the injury. P3 mentioned that they look at the accident/incident reports periodically to see if similar accidents are occurring at the same class and if they need to follow some approach or take some preventive measures to stop the accidents from happening. P6 also uses the accident reports for similar purpose.

After service termination, many of the centers keep the files of the parent and children for a certain amount of time. P3 mentioned they store the file for at least 2 years while P6 was not sure how long they store the file. She mentioned they store their older files in another locked facility.

4.2 Childcare as improvisational practice
Information management varies within a single childcare; practice is situationally-determined and negotiated based upon contextual properties. There are rules and policies in place regarding how to collect, store, access, and distribute information, but because a great deal of activity in a childcare is unpredictable, such management requires improvisational activity that accords with the context. As a result, we find policy modification that is mostly reactive (instead of predictive) or unfeasible. And, we find members at all levels of the childcare management (all the way up to the director and owner) filling odd jobs to keep the ship sailing smoothly in times of chaotic breakdown.

4.2.1 Unpredictability of events
The daycare is a place of great complexity and dynamism—a breeding ground for controlled chaos. As both P1 and P4 say, there is no typical day as a director of a daycare, no predictable busy times or down times; every moment is a possibility for the unexpected. One researcher witnessed P1 get surprised with an unannounced inspection (which can be expected twice a year for established centers, and 3 times in the first 6 months for provisionally-licensed centers such as this one). Two of her observation sessions were cancelled—one because too many teachers were out sick, keeping the director busy hopping between classrooms, the other because the director took the day off on account of her daughter being sick. Another observation was cut short when the director had to suddenly leave to take her daughter to the hospital. During another observation session, P6 had to drive the school van. She said this was not a usual case. She prefers driving the van than to schedule other teachers at the last moment since it becomes complicated. In a subsequent session, she had a similar incident but switched places with another teacher so that she could be in a class instead of driving the school van. In other cases, both P3 and P6 went to the unattended front desk (which is usually attended) to assist a parent or visitor. When P1’s facility was being inspected on a previous occasion, she noted her anxiety when the files being audited were laid out across the floor and children were running in and out without a care. When students get sick at P1’s facility, the director has to tend to them in her office, which meant cradling a baby to sleep for a half hour with lights off and business talk pushed aside to keep the baby from crying. Another director picked up the role of cook when the regular called in sick. Both facilities have hosted graduate student researchers in the past and juggle those responsibilities in addition to their childcare duties. And, with up to 200 children enrolled in the daycare, there’s never lack of "special cases—someone new picking Beverly up, Brandy’s leaving early, Brent is out sick today, Brittany is on vacation for the next two days, and so on and so
forth. Let’s not also forget accidents and incidents and parent-teacher conferences, or all the calls coming into the daycare center to schedule these events or make other communications. In the first 5 minutes of P1’s observation, the director had interacted with 7 different people at different instances. P4 says she has difficulty handling all the distractions and getting her work done. P1 agrees, saying that she sometimes goes home almost in tears for having so much work incomplete after a busy day. With only 3 observations at each childcare, such a wide variety of activity is surprising and clearly a source of frustration for information management.

4.2.2 Reactive policy management

Because the day-to-day affairs can be completely reconfigured by the onset of unpredictable happenings, there are a number of breakdowns in activity that take place. When the breakdowns involve relatively regular activities, then adjustments to policy can be made, but these are all necessarily reactive. There is little hope of preventing breakdowns that are either at the most basic level or have not yet taken place in at least one example case. Furthermore, even when critical breakdowns do happen, there is sometimes no practical way to adjust policy to account for them because they are so particularly unique.

Of the first kind—breakdowns that encourage constructive policy modification—we can see an example in recent news at a D.C. childcare where a kindergartener that was supposed to attend an after-school activity was dropped off at the wrong bus stop and left to wander the streets crying (http://www.dcmetromoms.com/2009/10/trust-and-the-school-bus.html). New policies have been put in place to prevent another incident of the same nature. But these aren’t just activities that happen in the news. There have been examples at our two participating childcare centers, as well. P4 noted that a new policy has been added to check that children have actually been buckled into their child seats before leaving on a class trip; this was necessary after the adult driver failed to buckle the child into the seat that was provided. In another situation, an incident report was left face-down in a classroom and a parent decided to look at the report to see who had bitten his child; the policy with regard to incident reports has changed to require these reports to be folded and stapled shut to prevent unauthorized access. Although these are tight-knit communities, sometimes it is harder to make everyone follow all the procedures to properly conduct a task. For example, the following field note gives an example of a case related to waiting list where the director is describing the previous process:

Previously, the process of taking information from a parent for entering them in the waiting list was done by almost everyone in the center. It was a mess because they forgot to ask critical information like ‘contact information’ or the age of the child. Some even forgot to write down the date when the parent was listed in the file or communicated with them. So, when a spot opened up, they didn’t know who called first. Without the child’s age, they didn’t know if the spot was right for the child. (Observation 2, P6).

In response to these events, P6 made changes to the waiting list maintenance procedure so that only she can take the phone calls related to the waiting list and get information for the list. Reducing the group interference and taking control over the process was a way to make sure that the policies were strictly enforced.

Of the second kind—breakdowns that cannot lead to practical policy modification—we have observed at least three instances first-hand in our short observation period. In one instance at P1’s location, emergency contact numbers in the school bus had not been updated in the move that took place when this childcare center opened up a second location; a child was not found at the pick-up location and the parent could not be contacted to confirm that the child was not expected to be there. In the second, P4’s side entrance door was found to be unlocked and a teacher offered up an apology; of course, the childcare doors are supposed to be locked at all times to prevent the risk of an intruder. Finally, in P1’s facility, the licensing agent happened upon a number of violations, including a purse and a can of spray paint that was left within children’s reach, as well as a wall outlet left uncovered. With respect to violations regarding
unlocked cabinets, P1 noted in a conversation to another teacher “if you unlock it, you lock it” and the other teacher responded with a practical and understanding tone: “yeah, well—sometimes you just get overwhelmed.” In the first case, policy modification would be absurd since the situation is so incredibly rare: one childcare branching into another location. For the second and third examples, we are reminded that policies are only as robust as the habits of the humans that exercise them; to err is human, a fact that no policy can circumvent altogether.

4.2.3 Duty of childcare is shared at all levels
Finally, there is deeply-embedded sense of camaraderie and community when it comes to the responsibility of keeping the childcare running smoothly. Most every employee—from the owner down to the volunteer student teachers—has a hand in raising these children. While the owners and directors do have unique responsibilities from the teachers, there are often situations that cause the distinctions in their jobs to collapse. This is not surprising, in that those at the top of the management hierarchy at the sites we visited had extensive prior experience. P1 started out as a teacher and has worked her way up through the daycare system for over 15 years. As previously mentioned, when a child gets sick at P1’s location, the child is brought to P1’s office and then tended to (and entertained with baby voices, bouncing chairs, walking around, dry erase boards, and so on) by P1. And, when teachers need help in the classrooms, P1 steps out of her office and takes on the role of teacher. A teacher at this location caught the one researcher taking pictures of the doorway (with permission of P1, of course), and she stopped the researcher in the hall and gave her a very stern, accusatory questioning to make sure that she was authorized to be in the center. Here, we have a teacher assuming the role of the director—a gatekeeper—as she acts as a concerned community member. In P3’s center, they conduct a regular tour at the classes to check if the teachers need anything, despite the fact that each class in the center has a phone and teachers can call the front desk if they need anything. This practice acknowledges the unpredictable nature of a classroom and how community comes together to make it work. In one observation, P6 finds herself acting as van driver for nearly an hour and in another session she tells the researcher that she may have to go to a classroom that is short one teacher during the afternoon. At P4’s location, when the cook called in sick, P4 had to step out of her office and devote herself to kitchen duty; the researcher doesn’t know who became cook when the director had to suddenly leave work and the observations session was abandoned. Finally, when the researcher arrived for what was to be the third observation at P1’s location, P1 cancelled on the spot because she was so busy filling in for sick teachers in the classrooms.

Unpredictable events, which are addressed by reactive policy management and shared childcare duties, all bring to light the improvisational nature of childcare activity; there may be predefined plans for a number of situations, but real life happenings have no trouble getting between and around these well-formed ideals.

4.3 Ideal Practices vs. Situated Gatekeeping
Much in the way of Lucy Suchman’s notion of plans and situated actions, childcare centers may have official policies, but the actual implementation of information management practices is deeply dependent upon the moment-by-moment context of activity (Suchman, 2007). This fact, however, does not preclude these centers from creating idealized information management policies (Bucciarelli, 1994). As we see in more than a dozen examples that follow (yet still a surprisingly small sample of all those that we witnessed in the field), several incidents directly contradicted the information security practices that were identified by the directors. Policies serve as references and are appropriated according to community and personal interpretations in their application.

All daycare directors in the centers we observed reported that their policy is to keep their office doors closed and locked and the filing cabinets locked whenever they were not in their offices. Doors to the daycare are also supposed to be locked at all times and only unlocked conditionally to let employees,
guests, children, and guardians in and out. However, in P4’s facility, the door to the daycare was found mistakenly unlocked (and was locked thereafter). In P6’s facility, the door was on two different occasions not only unlocked, but also wedged wide open with the director’s knowledge and left unattended during the busy time of the day when parents and children were coming and going. Both P4 and P6 left their offices for nearly an hour, but did not close or lock their doors (P6 actually left the building for this time, while P4 was about 100 feet down the hall from her office inside another room). These same two directors were both found to have unlocked filing cabinets during this time.

At P1’s location, an unannounced visit from the Virginia Department of Social Services (VDSS) licensing agency was witnessed. During the inspection, a cabinet with hazardous materials was found unlocked and a teacher’s purse (which may have contained medication or other hazardous materials) was placed in a child-accessible location; at least 3 more violations were noticed by the licenser that was performing the inspection, but none of them were written up according to VDSS policy. For one of these violations, P1 later said that the licenser assured that she would not report it “as long as... you don't let me physically see them.” The same licenser also expressed that she gives preferential treatment to the childcare centers that are more “diligent... as per say some people who want to open but they don't have their ducks in a row and they do it scatter-brained. That's very difficult for us and we tend to—I mean, I didn't have to come out, quickly [as she did to inspect P1’s facility].” She finished with: "yeah, but you know these are good folks, doing good work." P3 suggests that this particular licenser (who does inspections for her facility, as well) does, indeed, have a more lenient application of policies than other licensing agents:

I guess there is some variations on [licensing] anywhere you go. Umm, I know my licensing agent is not the one that my friend Tammy has in Dublin. And she is being written up for things that my inspector does not write me up for. Umm, you know—umm, because, my inspector was a childcare director at one time, she has done my job. So she tries to be—she reads the standards, she follows them, but her interpretations—they are—the standards sometimes are left open for interpretation, which can—there are times that my friend went toe-to-toe with her inspector because she doesn’t agree with her version of what it said.

At P4’s location, all visiting researchers are required to sign in on a sheet. When the researcher notified P4, she said she would have her sign in later, but she never did. And, the researcher wasn’t asked to sign in on any of her other visits. Office doors and cabinets that are supposed to be locked when nobody was present were not locked at both locations. Similarly, P1 said that it was policy that the spiral bound notebook with sensitive children’s information never left the office, but twice teachers were seen taking the notebook out of the office (though, perhaps they remained within view of P1 through the open door and large window that takes up most of her office wall).

A teacher came into P1’s office and asked for some information about the children. When the teacher learned that the information wasn’t in the black box (a box on the edge of the director’s table containing emergency contact information for all children), she said “can I dig?” (an informal phrase that suggested that this is not the first time she’s asked for this permission) as she directed gaze towards the filing cabinet that teachers are not supposed to have direct access to. P1 responded quietly, tersely, slowly, and with strain in her voice (in a way that suggested that she was being more protective of the information on the researcher’s account): “no, I will have to do that for you.” The teacher had a flabbergasted expression on her face and paused for a long while before speaking again.

As a final example, there was a critical breakdown of policy at P1’s facility with regard to school-age bussing. When children are bussed by the childcare to and from elementary school, there is a list of which children are expected to be picked up from the bus stop and a list of emergency contact information on the bus in the case that an expected child is not found at the stop. If the child is not present, then the bus driver must contact those on the emergency contact list in order to confirm that the child is not supposed to be picked up before leaving the stop. At P1’s location, the emergency contact information for a child that was expected but not found at a bus stop was not properly updated. Because the mother of this child
was a teacher with the childcare, the bus driver called her cell phone (presumably as listed in the driver’s own personal cell phone listing). When the mother did not pick up the phone, the bus driver called another teacher at the childcare to ask for her coworker’s (husband’s or home phone) number. This person did not know, and so handed the phone to the assistant director, who then walked across the way to P1’s office to echo the question to her. P1 did not know, and suggested calling yet another party to find the number. The mother was finally contacted and it was discovered that her child would no longer be riding the bus on Tuesdays. This critical breakdown of policy and the internal network of people that worked to rectify the mistake show how a childcare can be non-compliant with policy and just how many people can become aware of a situation through peripheral involvement.

These incidents suggest that ideal practices are just that; they are acted out in ways that vary with the context. Despite variation, and thus vulnerability to information security breeches, a number of information security techniques were exhibited by directors. For one, information that was verbally communicated was manipulated by managing volume, obfuscating meaning, negotiating to speak later, or not saying anything at all; we call this internal gatekeeping because it entails guarding information that is inside the mind as opposed to out in the physical environment. External gatekeeping, then, entails the management of physical information and takes place through altering the spatial, visual, and social accessibility of information

4.3.1 Internal Gatekeeping

When in conversation, the director and the parties they converse with manage who gets to hear which information and how much they understand what it means. As an observer, the researchers were often the people who were being kept ‘out-of-the-know.’ One of the obvious tactics was to whisper. This happened on several occasions at all locations. In P1’s office, the licensing agent exchanged a series of whispered statements with P1. These came after the licensing agent winced at the sight of what she later identifies as a past employee. The whispered statements were clearly about this person (e.g. “are you considering that staff?”, “just be focused, diligent”, “keep an eye out”, “the word ‘slacker’ comes to mind”, etc.) The same sort of behavior was seen when P4 carried on a 30 minute conversation with a coworker that was almost all in whispers and mostly inaudible to the researcher. The two also moved in close to one another and directed their voices to the other to make sure they could hear and the researcher couldn’t—for the most part. The researcher did hear some phrases that allowed her to determine that the issue was that one person is getting much lighter workloads in comparison to P4. Other information that is perhaps regarded as less sensitive or more appropriate for the audience is readily passed through the childcare without hushed tones. At P1’s facility, news of a child—Betty—that was to visit that day spread like wildfire through the center: her planned visit was written on a note for P1, someone came in and asked her about whether she had seen the note, when Betty arrived there was a conversation in the hall with P1 and a number of others, and when the owner passed by, P1 alerted her that Betty was currently visiting. Also, when the phone number incident took place at P1’s facility, at least 4 people were contacted and asked for the number (meaning that those 4 people probably learned about the incident). Finally, when the researcher overheard a phone conversation that discussed a child’s enrollment, P1 preemptively explained:

I was thinking about this while I was talking to Ellen—[you were] probably like ‘why are you telling this person about a child coming over?’ One of the little girls that came in to visit, Ellen is her teacher over there, so that's where the comment of 'oh, so you're taking one of our kids' [came from]—that was with her teacher hat on, then she slipped her mama hat on.... Sometimes conversation is much different depending on what parent it is.
Other tactics, like obfuscating spoken information, negotiating to speak later, not saying anything at all were also used. During one observation, P6 answered a phone call and went to a corner of the center, away from the researcher to make the conversation inaudible. In P3’s center, the office assistant was conducting a ratio count on the speakerphone when a teacher started to describe a problem. She immediately picked up the handset, presumably so that no one in the room could hear the problem. The whole time she was on the phone she did not talk much, making it harder for anyone to guess what went wrong in the class. One researcher was explicitly asked by a director to stay out of the office while she was making a closed-door call to a parent.

4.3.2 External Gatekeeping

External gatekeeping refers to spatial, visual, and social tactics used to maintain information security. Spatial tactics include putting physical information behind closed-off buriers. For example, P1 tucked sensitive information towards the back, in a file folder, behind a drawer, in a far corner, in an office—not only is the information spatially segregated from normal traffic flows, but it is also nested within a series of spatial buriers. Sensitive, semi-accessible information (the black box mentioned earlier, as well as a “message board” notebook with names of students that needed to be picked up at the bus stop that day) was kept on the corner of P1’s desk for teachers to examine before leaving to pick up children from school. In P4’s office, a file folder organizer was mounted to the front of her door and contained confidential emergency contact forms for teacher access only.

All of these spaces were also places, meaning that there were socially-constructed notions of what ought to take place with the information in certain spaces (e.g. only teachers know that this information can be accessed by them under certain conditions, and no one other than the director and their assistant can access the file cabinets located deep in their offices) (Harrison & Dourish, 1996). Even subtle cues about where coworkers are usually allowed in the office were used to spatially inhibit access to the filing cabinet, which—much like that described in (Dourish et al., 2004)—was located behind the line of the director’s desk on the far side of the office. In this way, information is kept safe through social means.

Finally, the extent to which items were visible was used as a way to manage security. As with the note in the back of the file folder, the director did not think that it would be as accessible to parents because, although she is not hiding it, she’s “just not making it 100% visible.” As information becomes more appropriately public, it is placed in more visible spaces (for example the sign up sheets and daily reports of activity placed on the doors of classrooms at facilities of P1 and P4). Visual tactics were also used proactively to guard against security threats (information and otherwise) in the way of numerous windows into key activity areas. Three of the four observed directors had large windows (one of these was a one-way mirror) that allowed them to peer out towards the entrance of the daycare. Each childcare center had some sort of locked front entrance that allowed returning guardians to use a key of some sort to enter and allowed guests to ring a bell for assistance. The windows played a key role in identifying visitors and managing access to the building. Unrecognized guests were questioned upon entrance. Even as the researcher entered P1’s building, she felt compelled to identify herself and her purpose to the directors that could see her enter through their windows and whose office doors were just beyond the threshold of the inner door entrance.

4.4 Asymmetries between Parents and Directors

As parties on either side of the customer / service-provider divide, parents and directors have different goals, knowledge sets, and authorities that translate into asymmetric awareness, access, and control of the child’s information. Parents and directors have conflicting interests, which can be manifested in communication breakdowns and lead different levels of access to information due to a controlled access environment. Another interesting side-effect of the inherent role distinctions of parent and director is the level of expertise that the director gains in the process of mass file management.
4.4.1 Conflicting Roles/Interests

Parents and childcare directors might both be responsible for raising the same children, but there exist a number of distinctions between their goals, knowledge sets, and authorities that keep them from equal grounds. Directors P1 and P4 both mention that the childcare’s purpose is to do what is best for the children. Ironically, while directors and parents share this desire to keep children safe, there are a number of unique particular concerns that lead to incompatible activities. For example, P1 indicates that parents teach their children how to press the green button that unlocks the front door of the daycare, which may be a security risk. And, a licensing investigation confirmed that on one incident parents let a child not their own out of the playground and then out of the childcare main entrance such that the child gained access to the street. P1 reminded a parent not to put the name of the childcare on the access card for the front entrance, which suggests that she is aware that parents are not always looking out for the security of the center. At another childcare center, P4 explained how one parent looked at the incident report of the child that bit his daughter to find out his name, a transgression for which the director scolded the parent (because, as P4 noted, it is both against policy and against the best interest of the child). P4 also identified a parent that neglected to strap a carpooling child into the provided car seat. The conflict of roles and interests can perhaps be seen best in the situation when the parents are suspected of child abuse—regular notes are taken to document the possible abuse and these are stored away (in places where parents either cannot or will not likely find them) before reporting to the VDSS. The ‘us versus them’ mentality that can sometimes arise when these misalignments take place was summed up well by the licensing agent and with agreement from P1: “burnout rate is high in daycare, but it’s not the children... it’s the adults.”

4.4.2 Communication breakdowns

Effective communication between parents and the childcare workers is difficult because, as explicitly stated by P4, “parents are busy and juggling a lot.” The childcare tries to cope with these communication breakdowns by having several forms of written communication: backpack mail (handouts that go home in children’s backpacks); sign-up sheets, flyers, monthly newsletters on classroom doors; emails; announcements at socials and meetings; hallway poster boards with flashy arrows and “read me” signs; and so on. Despite all of these communication techniques, parents still regularly miss the message. Several times during the observation, parents had forgotten to let the child care know that their child was not going to be a bus rider—even though this communication breakdown costs the parent $5 per occurrence. Another example from P4 makes communication seem like a hopeless case:

In the blue room, they tried to get photographs, they wanted family colleges, and I think they finally got up to about 50% participation. That was after, you know, a face-to-face transition meeting, they gave them the form, you know 'we just want to make a collage, we want to get some family pictures up,' a couple newsletters you know reminding them, and then at the parent meeting they reminded them. And, they were like 'we don't know what else to do, Kathy.' Well, just put up the ones we have.

4.4.3 Controlled access environment

One important distinction between parent and director is the degree of autonomy with regard to the contents and accessibility of the child’s manila file—who gets to access what information in which context? Several directors explicitly state that the files with children’s information belongs to the parents. For example, P1 says that “ultimately, [the parents] own those files, I mean, that's all their information.” However, law dictates certain practices with regard to file management, namely that the original file must reside at the child care and that a release form must be signed before sending the file to another child care in the case of a transfer. It seems to be common practice that parents can request to see the file in the director’s office and can receive copies of the information in the file (except for P10, who said that she’d prefer for parents not to view the files because they are laden with sensitive notes). Interestingly, (as with P10) directors sometimes place information in the file that they do not intend for parents to see. For example, P1 maintains records of potential child abuse at the back of the file—“it's not that we're hiding it
necessarily, but we're just not making it 100% visible, if that makes sense.” The fact that parents likely view the file in the office with the director present (as was the case with P3) could—through socially-constructed conventions—encourage parents to rush and exhibit an explicit information need. P4 also keeps sensitive information about parents, but it is stored in a completely separate folder that parents are not allowed to have access to.

P3 described one case where the parent demanded to see the child’s records. She asked him what exactly he was looking for and he said he cannot deny of the information. Although he wanted to see the records, the director asked him for the specific piece of information that he wanted to see; he said that he wanted to see his child’s attendance. Instead of showing him the attendance sheet, which had the attendance information of several other children included, the office assistant was asked to make a new spreadsheet with the last four months of attendance for the specific child. The parent is this limited to a specific timeframe of attendance and must wait several days before receiving the requested information. The accounts given by this director and others suggest that parents come into the childcare to request and view or receive copies of files (though we saw nor heard any evidence to indicate that phone call requests couldn’t be made, or that mailing files to parents wasn’t done). This means additional travel and time overhead than would be if the information was locally available to parents (e.g. on a website). Also, directors’ accounts implied that parents were to view files in the director’s office (though, again, we heard nor saw any explicit statement otherwise). And, in some situations what constitutes information that the parents can see and information that they can’t varies (although, in practice it seems that this information is always off-limits due to social conventions). All of these enforce a controlled access environment for parents and may result in affording them less control over their child’s information than they might have otherwise.

4.4.4 Expert file management

Because directors have more access to and responsibility for the manila file than do parents (and especially because they manage dozens if not hundreds of files that reflect diverse circumstances), there exists a gap in expertise; directors are much more familiar about what is in the file, how long it is kept, which laws govern the file contents, etc. P1 and P4 both explained almost completely the contents of the child’s file from memory—P1 even spouted out the color of the paper that each of five forms is printed on, what the title of the form is, which information is on it, and what the information is used for. P1 makes certain that she explains the forms to the parents as they are enrolling:

> When we sit down and enroll a child and we're ready to hand over paperwork for completion, we try to explain that entire set of paperwork because it is confusing. It's a whole lot of information to write down. So, we explain what it is.

The directors also know the legal requirements of the information and explain these requirements to parents when they are confused:

> Sometimes they don't fill out the form correctly, so I go up to them like 'k, so you're saying the director can't look at that, that means I can't prove your paperwork, can you please understand that my role is this—to make sure your child has everything they need to be in our school, that they've received immunization, they are who they are—I'm not giving it out,' then they're OK with it. (P1)

> You have to make sure parents are well informed because attorneys don’t always tell them that information. And that’s kind of our job to make sure they understand clearly what we have to, what laws we have to follow. (P3)

These examples show the directors taking on a teacher-like role and walking parents through the intended use of the provided information along with what rules and regulations are in effect with regard to that information. One director even takes it upon herself to remind parents that it is time to vaccinate or
immunize their children based upon the immunization records contained in the child’s file; this takes a task that is usually in the hands of the parent (that is, the task of remembering to get immunization shots on time) and places it in the hands of the director. One director, P4, even notes that she can remember certain information from the file and rely on that information to inform unexpected situations:

There is this form that the parents fill out that, it just gives them a history for the child from birth until they enter our program, so if they are observing some things in the classroom—and I do read those, and I'm pretty good at remembering the key pieces that are in there—so I'll say 'I read something about that' that the parent included in their folder.

From these examples, we see that not only are the directors intimately familiar with what’s inside (and what’s outside) the child’s file, they also know some of the child-specific information, how the file will be secured and eventually destroyed, and even use the information in the file to take over some of what may be considered to be the parents’ responsibilities.

5 Discussion

The data presented above can serve as a rich basis from which designers can work and discussions can be had about the digitization of our sensitive information. In effect, the data is itself the core contribution of this paper. The hope is that the richness of description can give the childcare experience to audiences beyond those that are actually able to become embedded in that environment. We refrain from taking the traditional route of identifying implications for design as a matter of respect for the complexity of the observed situation and the necessary situatedness of the design activity (Dourish, 2006). Instead, we provide descriptions of a small subset of the important differences between the worlds of digital and human information management: the difference between sensibility and regularity, between digital and physical, and between centralized and decentralized information management.

5.1 Sensibility vs. Regularity

The first of these is the difference between the regularity of computer information management systems and the sensibility of human information systems (a topic similar to but a superset of the notion of “assurance vs. trust” in (Flechais et al., 2005)). We saw in the childcare centers that improvisation is key to managing the day-to-day complexity and unpredictability of discordant events. This results in security measures that are most often created with the benefit of hindsight, makeshift shuffling of duties to respond to emerging demands, and a number of undesired VDSS violations. This chaotic environment combined with the variable, negotiable behavior of humans makes information security a dynamic act. As one example, P1 described when she once had dozens of folders strewn about the carpet of her office in the initial weeks the childcare was open, and how the children would come into her office and she would worry about the files. Dynamic circumstances hence yield situations where security is sacrificed.

This insecurity through unpredictability is not, however, the situation for computer systems. Of course, (in the absence of bugs) computer systems that manage user data most often have deterministic, consistent behavior. While there is some research into adaptive systems that can react in response to certain contextual cues, there is evidence that these static elements of context are not adequate to produce rich, human-like behavior (Dourish, 2001). In the common case, the machine will always restrict access to the person with, for example, the correct user name and password and will always give this person access to the same files. This is not to say that there are not flaws with these mechanisms (e.g. username and password can be shared, stolen, hacked, and files can be “accessed” by an onlooker, and so on.) But, the difference is still drastic; no matter how the context of the information access varies (e.g. the reason the user wants to access the files), the information presented (or not) will be the same and hence will be consistently guarded against unauthorized primary access or distribution. On the other hand, the human information management system cannot boast this consistency. In human information systems, official
policies are not the same as instantiated policies; for example, P3 says that licensing strictness depends upon the agent, and the agent that was at P1’s location confirms that she gives preferential treatment.

And, information access can depend upon any number of factors, like the ready availability of the data and a human to process; for example P3 delayed a father’s access to his child’s attendance sheet until the assistant could remove his child’s data from the rest of the children’s information.

At the same time as regularity in information management is lost with human management, sensibility of information disclosure is gained. People have the necessary equipment to make human-centered judgments; they can use the particular contextual circumstances as a way to inform information disclosure (for better or worse). As seen above, the activities that take place in a childcare are often improvisational (see 4.2.2) and according to community or individual preferences (see 4.3). Furthermore, practices clearly do not conform to pre-defined role-based activities because the roles are interleaved. For example, P1 spreads the knowledge that Betty is coming to visit and shares information with a teacher about a student that she would not share with others. Instead, activities proceed from the “fluid and especially the simultaneous nature of these capacities in which one acts” (Dourish et al., 2004). This flexibility of policy with regard to human decision-making is what we refer to as sensibility. Sensibility can sometimes result in negligence (e.g. when the door to the childcare was found unlocked), but it is also characterized by the ability to be more practical and respond to changing needs (e.g. to allow a recognized parent in when she has forgotten her key, to identify the unexpected failure to buckle a child into a car seat and adjust policy accordingly, to call an extensive network of related people in order to find the phone number of Nancy’s mom, and so on).

Another important distinction is that in a childcare center, security isn’t just about preventing break-ins, its also wrapped up in the willing disclosure of information and in the accidental undermining of security systems (e.g. leaving the door unlocked, teaching children to push the green button, etc.). The childcare becomes a place of mostly false positives, and the information system becomes the place of mostly false negatives. When someone in the community needs time-critical information, humans can weigh the options and err on the side of information usability (e.g. by publicizing emergency contact information), as opposed to most computer systems, which are designed in principle to err on the side of security (e.g. (Pettersson et al., 2005)).

5.2 Physical vs. Digital

A second point of interest is that the digital and physical worlds have completely different mechanisms for security management. The physical world allows for security to be managed with such intuitive mechanisms as visible, spatial, verbal, and social accessibility. There are certainly technologies that play a role in this, but their functional qualities are often incredibly intuitive (e.g. a manila folder). Many security mechanisms are so intuitive that they are actually created by the users themselves (e.g. office spatial layout, hiding child abuse information at the back of a file folder, information obfuscation, etc.). These mechanisms draw on basic principles that are physically and socially intuited from a young age without formal education. This is not as much the case in the digital realm, where underlying security mechanisms are extremely difficult to grasp without formal education (Whitten & Tygar, 1999). Even the location of information with respect to client and server—the basic spatial landscape of the internet— cannot be understood by many computer users (Pettersson et al., 2005). Without understanding the basic mechanisms of digital security, simply using the security features without undermining them is difficult, and appropriation is rare if not impossible (due to either programmatic constraints or lack of education/comfort).

Dourish et al. come to a similar conclusion in their own paper: the “visibility of system behavior on their terms, or the lack of it, was often a reason that people understood whether something was secure or failed to realize whether something was protected” (Dourish et al., 2004). The suggestion offered by Dourish et
al. is to make security technologies “highly visible.” Another approach is to educate users about the underlying technology’s vulnerabilities (Sheng et al., 2007). Without either making the underlying technology more intuitive or providing accurate metaphors of their functionality, it seems that education is a requirement for improved security.

The digital-physical security mechanism divide renders users less able to make informed security decisions and leads to a sort of defeatism that is not seen as readily when discussing the physical world (Dourish et al., 2004). For example, the licensing agent observed at P1’s facility observed: “if somebody really wants on [my computer] they're gonna be smart enough to get on it, whether I have a nice long 12-letter multi-digit pass code or not....” The licensing agent goes on to suggest that the childcare information stored on her computer is not valuable and that even if a hacker did break into it, she would not be able to access the information because the applications that it is stored in are so hard to navigate. Finally, she states: “I don't do online banking, I don't trust any of that, I mean I just don't, I don't pay bills online, I don't do any of that because I don't trust that someone can't just come right in and scoop it up.” This is the testimony from just one person in the childcare information management structure, and we do not have parallel testaments from others, but at least this one account suggests a number of important possible issues for usable security: that users do not understand the enemy and, the value of the data that they are overseeing, are intimidated by the thought of having information that they do find to be sensitive on the web.

With regard to not knowing the enemy in a digital environment, this user seems to underestimate the skills of an information perpetrator (doubting that she can understand or circumvent obscure interfaces). Other possible misunderstandings are how a perpetrator might “get in” to the system (not spatially, as in through the front door of the childcare), how she might intercept data (not audibly, by literally overhearing a conversation), how she can be detected (not visibly, as in sitting down at the computer to find data), and how she might be dissuaded from stealing sensitive information (not socially, through social constructions of where one belongs, because there’s little in the way of a society that can find and report the perpetrator). Not only may the user be blind to these characteristics of a digital perpetrator (which are often fairly clear in the case of the physical perpetrator), but also, the user must learn a completely new way of understanding the digital perpetrator (e.g. the user must learn perpetrators need not be visible even when they are in the same “space” that she is). The user also may not understand, as the licensing agent, the value of the information that they are in ownership of. The licensor’s computer contained, at a minimum, the names and contact information for parents along with social security numbers. While this is not the valuable bank account information that she is unwilling to put online, she fails to recognize that this information is important for identity theft, or for spamming companies, and more. This lack of understanding of what might motivate the perpetrator is a continuation of the lack of understanding of the perpetrator’s means.

### 5.3 Centralized vs. Decentralized

The third and final point is the difference between centralized and decentralized information management. Within each childcare, information management can be viewed as centralized. That is, the manila files, wall-hung notes, spoken word, tacit knowledge, etc. containing information about all employees, parents, and children is handled by a small group of people (mostly the owner, director, and assistant directors, but in some cases the teachers) as opposed to the management responsibility being distributed to the information providers (the parents, children, teachers). Let us focus on only the information regarding children, due to lack of space. Instead of each parent having to manage the information for their own child, one director (and, in some cases, the various other employees of the center) manages the information for all children (as many 200 children at P1’s facility, and as few as 43 at P4’s). This means that the director becomes an expert at managing these files. For example, P1 named each and every sheet that goes into the child’s file by name and listed the type of information that is requested on that sheet.
She knows the laws that require the information to be collected and the timeliness with which they have to be updated (e.g. for monthly or yearly immunizations). And, she helps remind parents to get the required immunizations for their children. With regard to child custody issues, P3 explained that she has a responsibility to “make sure [parents] understand clearly... what laws we have to follow.” After all, as P3 put it, “that’s kind of our job.” The director therefore becomes highly knowledgeable about information management because of the number and variety (e.g. some children are foster children, have custody issues, special health or education needs, etc.) of cases she handles. Furthermore, the centrality of information management has bearing on the “sensibility” of a human information manager as described above; with a human as the access point for information, the parents can get relevant, convenient (verbal) information that they need without having to search.

On the other end of the spectrum, digital information management entails a decentralized information management approach without (outside of) the service provider. That is, the set of files that make up the personal health record are owned and managed by each patient individually. The immediate consequence of this shift is that management expertise is spread thin across the entire user base as opposed to concentrated amongst a comparatively small number of regional “hubs” (e.g. the director in the childcare example). Thus, each patient must independently educate themselves about the laws that are particular to their situation and do this in the potentially lonely setting in front of their computer (the same lonely setting that has been blamed for decreasing the sense of community amongst computer science majors at Virginia Tech). Increased accessibility to one’s digital files (for the computer-savvy) coincides with a decrease of accessibility to a human interface with verbal, contextually-relevant feedback. On the other hand, being able to access files in one’s own space and on one’s own time may provide a more thorough inspection; certainly, ownership is also decentralized. One danger in this decentralized management approach is that there is still a great deal of the population (especially the older generation) that does not accept the computer as secure enough for personal data management (as exhibited by the VDSS agent: “I don’t do online banking, I don’t trust any of that”). This is particularly worrisome, since this is precisely the population that will be in and out of health facilities for the next 40 or more years to come.

The centralized nature of information in the childcare has at least two important impacts on information privacy and security. The first is that the information is likely to be passed along to many parties (e.g. teachers) beyond the actual information provider. For example, while most parents allow their child’s teacher to see the information in the manila folders for their children, this does not prevent another teacher, substitute teacher, or student intern from overhearing information, seeing information that takes place publicly or is hanging on the wall, see semi-public information (like the “message board” on P1’s desk), and the like. This could not only put information in hands that the parent had not agreed to or is not approving of, but it also does not afford the parent any knowledge of where the information actually moves and what it is used for (beyond the “official” information policies). The second impact of the expertise that arises from centralized information management is that a security transgression of one child’s information can be learned from and used to further protect the information of all other children. In the case of P4, one child’s incident report was looked at by a parent other than the child’s own; this was discovered by the director, the parent was confronted, and a new policy put in place to safeguard against future incidents. In a decentralized system, the lessons learned by one may not so easily be shared and transferred to another, remote digital information management user.

6 Conclusion

In this paper, we have explored the halls of four childcare centers—what they do, how they do it, and most importantly, why. We have found that the dynamic, unpredictable nature of day-to-day childcare affairs renders improvisation a requirement. Ideal information practices are thus foiled by unexpected events and the resulting situated security measures hinge on various forms of politically-mediated gatekeeping. The dynamic between patient and provider is such that various asymmetries of information
awareness, access, and control exist. We have also seen how these findings may speak to the impending movement of health documents to the digital realm: the impact of trading personalization for electronic rigor, the difference between understanding and appropriation in digital vs. physical information environments, and the impact on expertise and ownership as we move from a centralized to decentralized model for knowledge management. We have often mentioned in this paper that the transition to digital knowledge management systems will result in “altered” and “lost” practices. Of course, others will say that we have gained a great deal in the transition, as well, and we have. But, we must be careful not to get caught up in the love of technology as we drive technological adoption, and not to underestimate the evolutionary and experiential expertise that we are working from in our physical worlds. This paper is simply another call to look at what it is we are displacing before we displace, and has provided the means to do just that in a rich information management setting.

References


