Situating the Concern for Information Privacy through an Empirical Study of Responses to Video Recording

David H. Nguyen, Aurora Bedford, Alexander Gerard Bretana, Gillian R. Hayes
Department of Informatics
University of California, Irvine
[dhn, bedforda, abretana, gillianrh] @ ics.uci.edu

ABSTRACT
In this paper, we present the results of an empirical study of perceptions towards pervasive video recording. We describe a commonly used model for understanding information privacy, the Concern for Information Privacy (CFIP) model, and present the ways that this model and its associated questionnaire can shed light on information privacy concerns about pervasive and ubiquitous computing technologies. Specifically, the CFIP model encourages analysis of data across four facets of experience: the collection of personal data, the risk of improper access, the potential for unauthorized secondary use, and the challenge of preventing or correcting errors in the data. We further identify areas not well handled by this model of information privacy and suggest avenues for future work, including research on how and when to notify people about recording technologies, awareness of data provenance and leakage, and understanding of and access to the data assemblage being created about individuals.

Author Keywords
Information privacy, video recording, CCTV, CFIP.

ACM Classification Keywords
K.4.1 [Computers and Society]: Public Policy Issues—Privacy.

General Terms
Human Factors, Measurement.

INTRODUCTION

Computing applications frequently require the collection of vast amounts of data, including images and video recordings. In particular, the class of applications known as capture and access [34] are built on the promise of usefully collecting and making available these data. Video recording technologies, in the form of closed-circuit television (CCTV) and others (*e.g.,* webcams, camera phones, digital cameras), are some of the few truly pervasive capture and access technologies in existence today. Studying these technologies can provide insight into the ways that the novel capture and access technologies currently being developed and tested by researchers might be experienced in mainstream use.

CHI 2011, May 7–12, 2011, Vancouver, BC, Canada.

The pervasive capture of daily activities through video recording can raise concerns for information privacy (*e.g.,* [22]). Studies of CCTV, however, have primarily focused on the effectiveness and public support of the technology (*e.g.,* [7, 12]). For example, Dixon *et al.* reported that most people accept the use of CCTV despite belief that it could be abused [7]. These studies are only a first step in exploring the complex nature of those concerns.

In this paper, we present results from an empirical study about people's perceptions of pervasive video recording. We build on Smith *et al.'s* Concern for Information Privacy (CFIP) model as a means for interrogating multiple dimensions of perception about information privacy and video recording [31]. Our work provides three significant contributions. First, our results indicate how people feel and make decisions about pervasive video recording. Second, we demonstrate how the CFIP model for understanding consumer responses to information privacy can be applied to ubiquitous computing technologies (*e.g.,* pervasive video capture). Third, we present issues drawn from our empirical data that enrich and augment the CFIP model.

RELATED RESEARCH

Public opinion researchers have employed surveys to monitor overall levels of public concern for information privacy [8]. These surveys ask broad questions, such as "*How concerned are you about threats to your personal privacy in America today?"* However, these surveys result in a paucity of evidence for the specific dimensions of concern. In response, Smith *et al.* developed a model to measure individuals' concerns about organizational information privacy practices—CFIP [31]. The associated CFIP survey instrument has been adapted for and used in other contexts outside of organizational usage of personal information. Malhotra *et al.*, for example, used a modified CFIP instrument to understand Internet users' concerns for information privacy [23]. However, the CFIP model has not previously been applied to Ubicomp technologies, such as pervasive video recording.

Prior research has demonstrated the efficacy of drawing from models of privacy in other fields for use in design of Ubicomp systems. Palen and Dourish first applied Altman's privacy framework to describe privacy as a boundary negotiation process [28], with Lehikoinen *et al.* later

extending this framework to Ubicomp in particular [20]. Hong and Landay described risk models as a means for understanding privacy in Ubicomp systems and created a toolkit for developers to support privacy-sensitive design [13]. Similarly, Iachello introduced the concept of proportionality as a principle to guide the design of Ubicomp technologies and developed the associated Proportionality Method for designers [15]. Langheinrich used fair information practices as the basis for privacy design principles in Ubicomp [18]. However, these prior works do not tease apart the issues related to different dimensions of information privacy concerns. Thus, in this work, we turned to the domain of Information Systems, using the CFIP model as a basis to understand situated concerns about information privacy.

Particularly related to our work is Massimi *et al.'s* work on perceptions of recording technologies in general [24]. Both our study and theirs used the Day Reconstruction Method (DRM) to contextualize the inquiry [17]. However, their study examined all recording technologies; our study built on that work by focusing on and drawing out the nuances surrounding one particular recording technology—video recording. By using both DRM and CFIP, we were able to not only quantify participant concerns, but also use the CFIP model to provide a means for unpacking privacy-related concerns that Massimi *et al.* partially identified using DRM alone.

Additionally, previous work indicates that perceptions of and responses to tracking and recording technologies are highly contextualized (*e.g.,* [6, 24, 26, 27, 28]) and often impacted by the ways in which they are introduced (*i.e.,* as a tool to "help Grandma" not as a tool to "spy on an elderly woman"). Even if not explicitly told about a positive purpose for a tool, individuals may assume one, such as cognitive therapy for a person with a disability [27]. At times, this positive feeling about a technology may even come from something as simple as the name of the technology. For example, the Whereabouts Clock invoked in participants feelings of family togetherness over any concerns about location tracking, potentially due to its whimsical Harry Potter-inspired name [2]. End users make nuanced decisions about sharing private data based on a wide variety of contextual factors, such as knowing who wants the information, why, and at what level of detail [6]. These views of privacy support the notion of the privacy management process as highly contextualized and corroborate our interest in situated inquiry here.

A full review of the work on privacy within interactive systems is beyond the scope of this paper; instead, we refer the reader to Iachello and Hong's extensive review [16] and here have focused on only the most related works.

METHOD

Participants

Twenty-one participants (8 female) were recruited via both online classified advertisements (n = 12) and by word-of-mouth (n = 9). The participants represented a wide range of demographic profiles. Nine (42%) were between the ages of 18 to 29; six (29%) were between 30 and 50; and the other six (29%) were over 51. The majority of participants had completed university (71%) with yearly income levels reported in roughly even numbers across three brackets: 43% less than 30,000 USD; 24% between 30,000 and 60,000 USD; 24% over 60,000 USD (9% did not disclose).

Procedure

We used the DRM to elicit grounded and contextualized responses to video recording [17]. The DRM involves asking participants to recollect a full day (24-hour period) from the recent past—typically the day before. It has been used to study other surveillance technologies, such as cameras, browser cookies, and so on [24]. The DRM includes a combination of written recollection of experiences and a complementary interview. Participants were instructed to complete a time sheet for the previous day, crossing out any times they wanted excluded from discussion. No participant exercised this option.

After completing the DRM timesheet, participants were asked general questions including if they had any difficulty remembering certain time ranges and how typical their days were. Six participants reported having atypical days (*e.g.,* the previous day was a holiday). Recollected days included both weekdays and weekends.

Using the completed timesheet as a guide, we interviewed participants about each activity and time segment for details about the potential presence of video recording technologies. In addition, participants were asked to explain how they determined the presence or absence of video recording, the purposes of it, and who might have access to the data. The interview closed by giving participants an opportunity to discuss any general feelings they have about video recording systems. Two interviewers recorded and transcribed the interviews with participant consent. Interviews lasted between 30 and 70 minutes.

Participants also completed a questionnaire that included demographic questions and the validated CFIP instrument [31]. The parsimonious, 15-item CFIP instrument measures information privacy concerns along four dimensions: (1) *Collection* of personally identifiable data; (2) *Improper access* by people not properly authorized to view or work with the data; (3) *Unauthorized secondary use* of information collected for a particular purpose but used for another; and (4) *Errors* in collected data. The questionnaire measures information privacy concerns on a scale from 1 to 7, with 1 indicating very low concern and 7 indicating very high concern.

We counterbalanced the delivery of this questionnaire, administering it to half of the participants before the DRM and to the other half afterwards. There were no significant differences in responses between those two groups. Participants were compensated 40 USD for their time.

Privacy Dimension	μ (σ) this study (n = 21)	μ (σ) Smith *et al.* study #1 (n = 146)	μ (σ) Smith *et al.* study #2 (n = 183)	μ (σ) Smith *et al.* study #3 (n = 337)
Collection	5.54 (1.08)	5.28 (1.19)	5.11 (1.04)	5.45 (1.16)
Errors	5.33 (1.14)	5.36 (1.06)	5.57 (0.99)	5.46 (1.11)
Unauthorized Secondary Use	6.23 (0.74)	5.77 (1.22)	5.74 (1.14)	6.15 (1.07)
Improper Access	6.16 (0.96)	6.10 (0.89)	5.83 (1.01)	5.90 (1.01)
Overall	5.81 (0.72)	5.63 (0.78)	5.56 (0.83)	5.74 (0.86)

Table 1: Comparing Levels of Concern on a 7-point Likert scale (higher values indicate higher concern). There were no significant differences between participant responses and those from any of Smith *et al.*'s studies ($p > 0.05$ for all comparisons)

Analysis

By combining the CFIP model and the DRM, we are able to address two related issues. One, the CFIP instrument provides a quantitative measure of how concerned participants are in relation to traditional validated definitions of information privacy. Two, using the DRM, we can then compare the CFIP measurements with participants' everyday practices. Furthermore, we can use the CFIP model as an analytical lens to unpack participants' concerns and practices involving video recording, as seen in the data provided by the DRM.

Using the four dimensions of the CFIP model as an initial coding scheme, two researchers independently coded and analyzed the transcribed interviews. Additional passes expanded the coding scheme inductively along each of the four dimensions that were coded in the initial pass. The intent of the subsequent passes was to unpack Smith *et al.'s* formulation of the concepts of collection, unauthorized secondary use, improper access, and errors. These subsequent passes gave us a more nuanced understanding of the four broad dimensions of concerns as they manifested in the situated data, demonstrating how the model needs to be expanded to account for novel interactive technologies.

RESULTS

Overall concern as measured by the CFIP instrument is high, but not significantly different from Smith *et al.'s* sample populations (all p-values > 0.05; see Table 1) [31].

In comparing the dimensions with each other (see Table 2), collection and errors were not significantly different from one another, nor was unauthorized secondary use significantly different from improper access. However, responses to collection were significantly lower than responses to unauthorized secondary use and responses to improper access (respectively, $t(40) = 2.24$, $p = 0.02$, two-tailed t-test; $t(40) = 1.98$, $p = 0.05$, two-tailed t-test). Responses to errors were significantly lower than responses to unauthorized secondary use and responses to improper access (respectively, $t(40) = 3.02$, $p = 0.004$, two-tailed t-test; $t(40) = 2.54$, $p = 0.02$, two-tailed t-test). In other words, concerns for unauthorized secondary use and improper access were higher than concerns for collection and errors.

In the following sections, we present the results from our qualitative analysis of the interview data as they relate to each of the elements of the CFIP model: collection, improper access, unauthorized secondary use, and errors. When used together, CFIP and DRM enabled us to better understand people's perceptions of video recording technologies. We used CFIP and DRM to break down generalized concerns in a contextualized manner. The results from analysis of data collected through the DRM provided a situated understanding of people's perceptions. CFIP provided a model to unpack that situated understanding. In particular, CFIP and DRM used together provide a detailed opportunity to deconstruct the misalignment of privacy behavior that has been seen in previous research (e.g., [5, 26]). Specifically, although concern for information privacy was reported as high, the DRM was able to show how these concerns were nuanced and how they could be played out in everyday use.

Collection

Smith *et al.* use the term *collection* to describe concern over the amount and quality of personal information being collected about consumers. The CFIP questionnaire operationalizes these concerns in two ways. First, people might be concerned that organizations are asking for and collecting too much personal information. Second, people may express concern that too many organizations are requesting and collecting this information [31]. In our data, concerns about collection focused on how resources were used and how participants were notified and asked for consent.

Using the CFIP instrument, participants responded with a mean of 5.54 in the collection dimension (sd = 1.08),

Subscale μ (σ)	Errors 5.33 (1.14)	Unauthorized Secondary Use 6.23 (0.74)	Improper Access 6.16 (0.96)
Collection 5.54 (1.08)	p = 0.56 t = 0.59 df = 40	**p = 0.02 t = 2.42 df = 40**	**p = 0.05 t = 1.98 df = 40**
Errors 5.33 (1.14)		**p = 0.004 t = 3.02 df = 40**	**p = 0.02 t = 2.54 df = 40**
Unauthorized Secondary Use 6.23 (0.74)			p = 0.80 t = 0.26 df = 40

Table 2: Comparing Levels of Concern Across Subscales

meaning they were generally concerned about the amount of personal data being collected about them. However, when explicitly asked to consider video recording—a potentially rich source of personal data—they expressed nuanced, multi-faceted rationale around when collecting video data was acceptable and when it should be prohibited.

One of the primary reasons repeatedly expressed for tolerating, or even embracing, pervasive video recording is the benefit these kinds of technologies can provide.

> *I feel like with the added security that there's a camera there... If somebody comes into the restaurant with a shotgun or something and holds us up… we'll get the money back because we have it on video tape.* (P08)

This kind of cost-benefit analysis echoes Westin's notion of privacy pragmatism [35], Iachello's proportionality method [15], and Hong's risk models [14]. As P19 noted, *"We're going to lose some privacy but we're going to get also other things out of it…"*

Notification and Consent

Although participants often reported being comfortable with collection of video data, they described being most concerned about recording activities to which they did not consent prior to the recording, particularly when at home or in another space generally considered to be "private." Of course, the first step to consenting to recording is to become aware of it.

> *…I really think they need to let people know that they are being monitored, or any place that you enter so you still have the choice… (P11)*

Notification of recording can occur in a variety of ways, such as seeing the camera itself, observing a video feed from the camera on a large display, reading a notice at the site of recording, or being notified of recording prior to installation. However, participants reported becoming acclimated to both the recordings and notification about them. Furthermore, in public places, people described having limited concerns about video recording despite substantial concern over collection of data generally (as indicated by the CFIP instrument). Typically, this tolerance stemmed from both acclimation over time and a general lack of awareness of the recording activities.

For example, referring back to a therapy training program during which sessions were video recorded, a school counselor commented:

> *So at first it was really nerve-wracking and you just feel like you're going to be judged by people watching, but then after a while it was just commonplace. And you just became comfortable with it. (P21)*

At the same time, CCTV has become so integral to stores that it may be viewed as essential to remaining in business.

> *…it has become so commonplace it's not something I think about consciously. In other words, yeah, its there and you move on and who cares? And if it's not there, I probably just wouldn't even notice it's not there. (P10)*

The need to notify people in an unobtrusive way that still garners their attention and consideration is a significant problem for HCI. In particular, as more recording happens in mobile and ubiquitous computing applications where the technology is designed to "disappear" into everyday objects, notification will become both more difficult and more important for user adoption and acceptance.

Required Resources

Perceptions of the resources required to collect and store large amounts of data can complicate considerations about recording. For example, a project manager who expressed concern about data collection in the office was less concerned about collection of data in the home because it was "expensive" and "useless"—therefore improbable:

> *…recording devices are expensive and cost money… The most interesting thing they'll hear is me feeding the cat or something like that. Therefore, it is useless. (P10)*

Concerns can be raised over the potential for databases to combine personal information from various sources, creating a "mosaic effect" [31]. This issue is present throughout the literature (*e.g.,* [4, 19]) but came up very little in our data. One notable exception to this trend was an individual whose office workplace had extensive surveillance to monitor employees. She noted that she was careful about the departments she visited and how often she went to the bathroom based on the idea that her employer could assemble information from all of the various cameras to provide a comprehensive view of her day.

Improper Access

Smith *et al.* use the term *improper access* to describe the set of concerns around who can and should access the data, according to the individual's beliefs and concerns. This issue inherently brings up technological issues (*e.g.,* being hacked either internally or externally) as well as policies and social norms. The CFIP questionnaire operationalizes these concerns as deficits in the willingness or ability of organizations to prevent unauthorized access, including the often-expensive protection of databases and ensuring appropriate access control to prevent unauthorized people from accessing personal information on their computers [31].

Participants expressed a mean response of 6.16 in the improper access dimension (sd = 0.96), meaning they were highly concerned about their personal data being accessed by the "wrong" people. However, in our interview data, considerations of improper access included accidental sharing, in addition to intentional or malicious sharing. At times, concepts of *improper* access also related to *unknown* access, in which participants struggled to describe who might have or want access and why. In this section, we detail the ways in which these concerns about improper access emerged.

Data Protection Policies

Typically, the protection of personal information has centered on a notion that only those who "need to know" may access the data [21, 29]. This trend in organizational policies echoes the views expressed in our data.

> *I don't think that anyone else would necessarily need access to those cameras or to that footage, because if their sole purpose is to regulate traffic, I don't think that anyone else needs to have access to that information. (P05)*

Others suggested these large organizations might customize access controls based on their personnel:

> *…that type of information and data is supposed to be protected… So, you can't… have a lower-level employee who is looking at the data and like, stalking someone. … there should be a safeguard or a hierarchy of who gets access to that information. (P14)*

> *…you wouldn't want to trust [reviewing records] to just a regular store worker, especially since the turnover rate on retail people is so high. (P02)*

This kind of thoughtfulness was most often ascribed to large organizations. One participant even described the notion that these policies inherently should become more sophisticated with the growth of an organization,

> *As you move away from a franchise or small business into larger corporations, they're usually far more advanced in privacy policy and who has access to what… let me rephrase that: should have. It doesn't mean they do. (P10)*

In smaller organizations, perceptions of data protection policies were often linked to other beliefs about the organization itself. For example, P10 described a particular store he had visited of which he thinks highly:

> *That store…it strikes me as a well-run business, so therefore, I'm taking that same leap that they are taking then certain precautions that a good business would. In other words, everything being consistent, I would guess that they would have very limited access, probably locked up in a manager's office. Literally locked. (P10)*

Within some organizations, trust and close relationships among the people in them can be considered adequate protection without specific policies. For example, in describing recording and broadcasting of church sermons for which there are no hard policies about data protection, a churchgoer nonetheless viewed herself as adequately protected based on the accountability to those with access to one another and to the church leadership.

> *They have a team that's their audio/visual team, and they're accountable to the person who works on staff…He's in charge of all the publications and things like that, and then they're accountable to the head pastors. So, there is a little bit of overseeing going on. (P20)*

Appropriate policies around data protection can benefit small businesses in other ways as well, such as the protection of the business from internal fraud. For example, P08 manages a restaurant at which a tape in the CCTV system can only record for the length of one manager's shift. To protect the data, the first thing each manager does when he arrives is

> *…put in the time you put the tape in and the time you take it out. You write on the tape the time that you took it out… and then after you have taken the other one out, you have to sign it. And put it in the safe, which is for videos. (P08)*

The policy of having the manager for the next shift replace the tape from the previous shift limits the potential for a manager to take identifiable data out of the restaurant, fraudulently replace a tape showing misconduct, and so on.

A particularly strong type of policy, legal protection of video data, can include the requirement for a court order, the inadmissibility of evidence in court, and laws surrounding libel and slander [1].

> *[No one else would have access to the records] without a court order or anything. Normal things that would apply to wire-tapping and things like that need to have court orders to be done. (P01)*

Leaking, Sharing, and Gossip

The most common concerns over improper access centered on the idea that another person, not present, could be hurt or offended by something recorded.

> *Sometimes we talk about some private information… so I would not want that disclosed…I would be very upset if somebody recorded it and then like, it leaked out to the people that we were talking about. (P18)*

The repercussions of this kind of data leakage may not be as severe as identity theft and other risks of improper access to personal data. However, improper access can ruin relationships and disrupt careers, which for many individuals are more "real" concerns than identity theft and other commonly described risks. For example, describing recording from a job interview, a university counselor noted,

> *It's hard to trust where that's going, and I don't want anyone to be hurt. Sometimes I might joke around, but … if the candidate heard that, or a student heard that, and then they told their friend, I'd just, I would be horrified, because I don't want to be hurtful to anybody. (P21)*

People work diligently to protect their reputations and present themselves appropriately in different situations [10]. Improper access to video records has the potential to break those expectations about who saw whom behaving in what ways with potentially negative consequences.

Uncertainty

Despite concerns about improper access, in many cases, people expressed ambiguity about who *does* have authorized access to the records. For example, in describing traffic cameras, P14 noted *"I'm assuming the Caltrans department, possibly the police, maybe California Highway Patrol. I'm hoping those are the only departments."*

Adding to the ambiguity over *who* can access records is the concern about *how* they might access them. Monitors in unsecured locations, such as a security officer's desk in the main lobby of a building or even mounted from the ceiling in a store to deter theft, are often used to view recordings. These monitors can be viewed and perhaps recorded surreptitiously using another video camera.

> *Obviously security [has access to the data] and anybody that would be walking by if it's not a closed station. I suppose anybody could look at the monitor. (P15)*

The laws and policies regulating access to personal information do not yet completely account for video recordings. For example, the Family Educational Rights and Privacy Act[1] in the United States requires that guardians of a child must be given access to all school records for that child upon request and that no such records will be given to anyone else without their consent. If video or images of multiple children are captured and stored at a school, it is not clear how the school is meant to handle the case in which the guardians of one child demand a copy of the image and the guardians of another refuse its release.

Unauthorized Secondary Use

Secondary use implies that information collected for one purpose is used for another. This kind of secondary use is central to argumentation about many recording applications in HCI, for example, any data mining application that uses data collected for one purpose to reveal connections that were not previously known. Likewise, it is common for corporations to find additional uses for data already collected, such as utilizing research data for marketing purposes [3].

When secondary use occurs without the permission of the person whom the data describe or without deidentifying these data, it is considered *unauthorized secondary use.* Unauthorized secondary use can be internal—access and use by a party internal to the organization that originally collected the data—or external. Both kinds of "information release" [32] can intensify concerns over unauthorized secondary use [33].

The CFIP instrument operationalizes beliefs about unauthorized secondary use in terms of agreement with two principles. First, organizations should not use personal information for any other use than originally intended without permission (internal). Second, companies should not sell personal information nor share it without permission (external).

Participants reported a mean response of 6.23 in the unauthorized secondary use dimension (sd = 0.74), meaning they were generally highly concerned about their personal information being used for unauthorized purposes. In this section, we describe the concerns people reported during interviews about internal and external secondary use, as well as concerns emerging from a lack of knowledge or understanding about how their data might be used, why their data are used, and the impacts potential secondary uses might have on how video data are collected, monitored, and analyzed.

Internal Unauthorized Secondary Use

Interview participants hypothesized about a variety of potential internal unauthorized secondary uses in which organizations that collected data might reuse it without permission. Participants often noted that it was unclear what the data collectors might do with these recordings after they were captured. For example, when asked about other uses of video recording in a mall, P14 posited that they might be used to *"count foot traffic and seeing how busy the shopping center is. I guess they could be doing racial profiling or something…"*

When participants described being more confident about the potential for internal secondary uses, these uses were nearly always attributed to the idea that employers and business owners might observe the activities of their employees. For example, as a shopper, P10 described how records from security cameras might be used in a store if he were the owner of that store:

> *I, as an owner, would like to see the interactions of my employees. I don't know if that's legal. I would have to learn that, but it would be good to see the interactions with the customers and how customers react to them, but other than that, I don't know how it could be used. (P10)*

As noted in the quote above, the legality and underlying ethics of such a choice are not always immediately clear. Particularly in public or semi-public locations like a store, the expectation of privacy might be so minimal that secondary uses, even those that are unauthorized, are not well protected under current law. Instead, corporate policies may be more likely to govern these kinds of uses.

Even in those places where employee surveillance is commonplace, however, these uses have often emerged from an infrastructure originally installed for security or some other purpose. For example, one participant described her workplace, in which surveillance is the norm:

> *…before, the intention was for burglary, if somebody is going into the building, but now, it's more for monitoring employees to see if they are doing something wrong… The company doesn't trust you. You don't feel good about it, because… they're using it against you. (P11)*

Although Smith *et al.*'s discussion of unauthorized secondary use referred to the repurposing of data, in the case of video recording and CCTV systems, the entire infrastructure can also be repurposed over time. For example, CCTV systems installed for security purposes in restaurants can be used to help recognize customers looking for service. This expansion of the definition of unauthorized secondary use is particularly relevant to HCI research, in which highly evolved infrastructures for tracking and

[1] http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

recording are currently being developed and may be put to a variety of uses in the future.

External Unauthorized Secondary Use

The intentional sharing or unintentional leaking of data beyond the organization that originally collected it constitutes external unauthorized secondary use. In our study, concerns were raised about particular parties who might gain access and use the collected personal information. There was also a general sense of "other" parties, in which that "other" gaining access would be undesirable. When probed about this kind of external access, however, many individuals reverted to a "need to know" articulation similar to the policies surrounding improper access, with the underlying position that protections would be in place to keep data from any external parties who have no explicit need to know this information. Furthermore, participants at times described being influenced by existing laws surrounding data protection that take a similar position: *"…being that Disney is a Fortune 500 company, they wouldn't want to be violating any of those laws." (P12)*

Of course, some of the most common concerns about external unauthorized secondary use were those related to identity theft. For example,

> *I wouldn't feel comfortable of them recording [financial transaction] just because I wouldn't want it falling in the wrong hands, to have my identity stolen or somebody tapping into my credit cards… (P08)*

Some individuals had specific people in mind from whom they would like data protected. For example, in describing video cameras in a classroom, a college student noted:

> *As long as they didn't show it to my parents, I'd be fine, because sometimes I sleep during class, and they'd probably get angry. (P13)*

In the cases in which specific "others" are of concern, it may be that respondents' identities are carefully crafted for those individuals (*e.g.,* a boss, parents, etc.) and that the concern lies in discovery of behavior outside of their expectations. In other cases, however, the issue at hand is the persistence of the activity, rather than its initial experience. For example, after describing his amusement at the idea of replaying embarrassing moments in his friends' lives, a restaurant manager was explicit in his desire not to have such moments replayed about him:

> *I don't want them to see my faults. That's a definite no. If I was able to, I'd erase it so that nobody else could see it. I don't want anyone to have ammo against me. (P08)*

Unknown Secondary Use

Although Smith *et al.* clearly delineate notions of internal and external unauthorized secondary use, in our data, individuals were often unsure what kind of violations might occur. Concerns centered on the fear that some unknown other would access the records for some unknown purpose: *"I believe that would be the main purpose. I would hope it's not some other purpose!" (P18)*

Similarly, once an individual had agreed to recording, even with only a vague idea of the primary use and the primary user of the data, objections arose to the idea of another use. In particular, after determining a logical primary use in situations in which the actual use is unclear, participants struggled to articulate other potential uses and therefore objected to these unknown secondary uses. For example, after describing being comfortable with traffic cameras for *"traffic and safety purposes",* P01 went on to describe disagreeing with other purposes, such as *"general surveillance that have no particular law enforcement use per se, just for spying on people who haven't done anything."*

When participants were unsure about the potential uses of the data, they also described being unsure of archival policies, analysis methods, and access practices.

> *If they're using it for marketing data, then I most certainly believe people are analyzing and studying it very carefully… if it's just for security purposes, then I think it's not studied as much as it would be for marketing. (P14)*

These results indicate that individuals may not yet understand the kinds of secondary use to which video recordings—and for that matter, other data streams collected by information technologies—might be put.

Errors

Smith *et al.* use the term *errors* to describe concerns that organizations are not taking enough steps to ensure the accuracy of the personal data they store and use. In the CFIP instrument, concerns about errors are operationalized as deficits in two areas: organizational investments in time and effort to ensure the accuracy of their databases and organizational procedures to correct errors [31].

Although there are examples of researchers—even Smith himself—describing the inspection and correction of errors as solutions for addressing these concerns (*e.g.,* [29, 30]), Smith goes on to describe how errors can be "stubborn" and "snowball in spite of such provisions" [31]. He asserts that these errors may be malicious or accidental, noting in fact that a large source of errors might be the presence of data that have changed or fallen out of date and thus should be deleted [25, 31].

From the CFIP instrument, participants provided an average response of 5.33 in the errors dimension (sd = 1.14), meaning they were generally concerned about the errors that could occur in the records about them. More specifically, in our data, individuals described cases in which expectations of the presence of data influence the required accuracy of those data. Thus, in this section, we describe concerns and expectations about accuracy in terms of both accidental and malicious errors present in both the presence and the absence of data.

Correcting Errors Using Video Evidence

Seeing is believing, as the old adage goes. Often video "evidence" is believed to be "reality." However, every video recording is selective in some way, whether it be the angle, the quality of the recording, or the control of when recording occurs and how long it is archived. Recording can enable the recreation of "truth" from video within "socially situated, historically constituted" bodies of practice [11]. Video records have the appearance of "realness," but without the extra context of lived experience, people construct a variety of explanations for any particular video record.

Given the potential for video to provide a kind of "truth" that other records are often perceived not to have [11], respondents described using video evidence to correct errors in other records. For example, when asked about the uses of video recording in a parking lot she frequents, P05 noted *"If someone's car was being towed because they didn't have a permit, but on the video it shows they have a permit, [they can contest the ticket.]"* Similarly, P08, a restaurant owner uses a substantial CCTV recording system in his business. He described being concerned about someone fraudulently filing a claim in his restaurant and how he might use the records in such a case:

> *Like somebody slipping, like fabricating a story about slipping in the restaurant and suing us while we have it on camera that they cause their own slippage… it serves as evidence.* ***To me, video cameras don't lie****. I mean it shows the date, the time, and it shows you were at a specific place at a specific time." (P08, emphasis ours)*

These kinds of beliefs in the relative infallibility of video recording may explain in some part why eight participants tested very high (6 or above) on Smith *et al.*'s errors dimension in general and yet reported in interviews less concern about errors that could occur in the video records specifically.

Reality-Based or Reality?

Concerns over accuracy of the interpretation of data in video records do, however, abound in our interview data. In particular, video records can give the appearance of a truth of sorts and yet be flawed. At times, these flaws can undermine a sense of safety that justice will prevail due to the recording. For example, although nearly every interview participant noted at some point that records can be used by police to oversee traffic accidents, prosecute criminals, and so on, P20 described a real-world example in which the video records were not of a high enough quality to meet her expectations:

> *A friend of mine was killed in a very serious accident that had a camera, and it didn't get anything. The person ran… it's still a little bit difficult to prove who's there. (P20)*

The potential for records that seem perfect on the surface to be flawed when interpreted also led to concerns about what might be ascertained from the video records and how actions might be interpreted by someone later, often out of context. For example, in describing behavior in a workplace that is heavily monitored, P11 noted:

> *… that's why we don't try to go to other departments, because you don't want them to think that you aren't doing anything. So, that can be construed as gossiping or wasting time, when they see you on the camera.*

Finally, in a world in which surveillance for the sake of securing our borders, trains, planes, and so on is rapidly proliferating, errors in video records or their analysis can have severe consequences.

> *I know that there's a margin for error…I am sure people have been detained because they look like [someone wanted for criminal activity]. (P15)*

Despite comments about the potential for errors, few participants described these kinds of severe consequences (*e.g.,* false imprisonment) or wanting to prevent video recording from taking place in most places outside their own homes. However, stories in our interviews resonated with reports of public surveillance projects being abandoned due to citizen concerns as well as consumer choices, such as boycotting a store. For example, P10 noted his discomfort with constant reminders of surveillance cameras in stores that make him feel distrusted: *"…if it's a place where all I'm reminded of is 'you could be a criminal', then I'd probably go somewhere else."*

The Absence of Nuance and Context

Video records can often be accurate in form and content but inaccurate in terms of how people perceive a particular occurrence or activity. Human judgment is filled with nuance, responses to contextual cues, and so on. These capabilities can be hindered when the records are created and acted upon without substantial human intervention. Most frequently, this concern surfaced from interviewees describing traffic and "red-light" cameras. For example, when describing a traffic citation his father received, P14 noted, *"…they gave him a ticket, because he ran the red light, but it was safe…I don't think he should have gotten the ticket just because it was a safe judgment…"* People are accustomed to discussing the nature of a traffic citation with the officer delivering it, and in many cases, convincing the officer to reduce the citation to a warning or some other lesser charge. Increasingly, however, the camera is the decision-making agent with which negotiation is impossible and through which citations are easy to issue.

> *Even when there's no one there, you're being filmed at an intersection, and it's one thing if you blew right through a red light or something that you deserve…but a lot of this persnickety little stuff—like, you didn't stop or you went through when it was yellow—I just think it gives too much power... (P17)*

Thus, although technically accurate, these records can create a mismatch between traditionally perceived nuanced

enforcement of laws and a new state in which laws are enforced completely.

DISCUSSION

Concerns over information privacy are "neither absolute nor static, since perceptions of advocates, consumers, and scholars could shift over time" [31]. Indeed, such shifts have been demonstrated repeatedly in the literature, including the shift from a particular population wanting to be notified about CCTV [12] to the same population not caring [7], as well as the continued rising levels in reports about general anxiety over information privacy [8, 35]. Similar to other populations who have been studied using the CFIP instrument, our results indicate that people continue to be concerned about information privacy as a general case. However, the way in which concerns about collection, unauthorized secondary use, improper access, and errors are articulated with regard to pervasive video recording technologies require expanded consideration of these dimensions of information privacy.

Collection. Our results indicate that collection of large quantities of video data is nearly assumed when outside the home or other private spaces in the United States. Similarly, search engines, tracking cookies, and other software accomplish substantial surveillance of online activity [9, 26]. This repeated exposure to data collection and an overall sense of continuous surveillance helps to explain why reported concerns for collection were lower than the responses to improper access and secondary use. When recording was not expected, people described wanting to provide informed consent. However, the first step of that process—being informed—requires improved awareness of what is being collected and how it might be assembled during long-term, large-scale collection. Participants described a general lack of awareness, suggesting the need to expand the CFIP model to gauge awareness and understanding of how and what personal information is collected. Furthermore, this issue raises open questions for HCI researchers and designers who seek to develop new models and mechanisms for informing people about recording and assessing their consent to that recording.

Improper Access. Concerns over improper access of video recordings were articulated by participants in terms of data protection policies for video as well as the kind of accidental sharing that might come from data leakage or uncertain security protections and processes. The lack of awareness about who has access necessitates expansion of the CFIP model to measure awareness and understanding of processes used in storing, processing, and disseminating collected personal information. As shown in previous work on location data, who has access to collected data impacts concerns regarding information privacy [6]. An open challenge for HCI designers and researchers, then, is to provide awareness of not only how and what personal information is being collected, but also who may have access to data invisibly stored on servers elsewhere.

Unauthorized Secondary Use. Participants described being concerned about both internal and external unauthorized secondary use of video data, most of which is unknown to the participant. The uncertainty over who has access and what they might do with the data indicates both a challenge of using the CFIP model in HCI and Ubicomp and a challenge for HCI designers and researchers to inform those recorded about the capabilities of these technologies. Additionally, the flexibility of these systems requires that the CFIP model be expanded to account for not only the reuse of collected data but also the repurposing of existing infrastructure and applications for other uses. Unfortunately, it is all but impossible to account for every potential, possible use of the personal information, infrastructure, and applications involved.

Errors. Finally, consideration of concerns over information privacy and video recording in terms of errors brings to light the ways in which the expectations of the infallibility of video recordings influences views on the acceptability of these records. In particular, expectations of the data to provide evidence and represent "reality" without the nuance and context of lived experiences may not match the potential for errors nor the capabilities of the systems themselves. Additionally, the notion of errors is not solely technical. Participants were also concerned about the erroneous interpretation of video recordings. In light of these challenges, the CFIP model should include a consideration of the understanding of the technical capabilities and limitations of Ubicomp technologies.

CONCLUSION

Application of the CFIP model to video recording technologies can enable understanding of the four dimensions of information privacy concerns: collection, improper access, unauthorized secondary use, and errors. However, the original CFIP model must be augmented to account for issues that emerge in Ubicomp technologies, particularly those related to pervasive tracking and recording, such as video recording. In this paper, we have presented an analysis of empirical data surrounding concerns over information privacy in relation to video recording. These results demonstrate that just as with other issues of information technology and privacy, respondents have nuanced and complex responses to these technologies. Furthermore, our results present a variety of challenges for HCI researchers and designers including how to inform and to educate end users and those who may be recorded as new technologies are created and how to present these technologies in ways that encourage adoption and use while still being informative about potential risks.

ACKNOWLEDGMENTS

A US Department of Education GAANN Fellowship to the first author has supported this research. This work was also supported by NSF grant 0846063. We thank Amy Voida, Steve Voida, and the members of the STAR Group for their comments and input on earlier versions of this paper.

REFERENCES

1. Andrews, S. *Privacy and Human Rights in 2002: An International Survey of Privacy Laws and Developments*. Electronic Privacy Information Center (2002).
2. Brown, B., Taylor, A., Izadi, S., Sellen, A., Kaye, J. and Eardley, R. Locating Family Values: A Field Trial of the Whereabouts Clock. In *Proc UbiComp 2007*, Springer (2007), 354–371.
3. Cespedes, F.V. and Smith, H.J. Database Marketing: New Rules for Policy and Practice. *Sloan Management Review 34*, 4 (1993),, 7–22.
4. Clarke, R. Information Technology and Dataveillance. *Communications of the ACM 31*, 5 (1988), 498–512.
5. Connelly, K., Khalil, A., and Liu, Y. Do I Do What I Say?: Observed Versus Stated Privacy Preferences. In *Proc. INTERACT 2007*, Springer (2007), 620–623.
6. Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J. and Powledge, P. Location Disclosure to Social Relations: Why, When, & What People Want to Share. In *Proc CHI 2005*. ACM Press (2005), 81–90.
7. Dixon, J.A., Levine, M. and McAuley, R. *Street Drinking Legislation, CCTV and Public Space: Exploring Attitudes Towards Public Order Measures*. Home Office On-Line Report, London, 2003.
8. Equifax Inc. *Harris-Equifax Consumer Privacy Survey 1992*. Equifax Inc., Atlanta, GA, 1992
9. Fox, S. *Privacy Implications of Fast, Mobile Internet Access*., Pew Research Center, Washington, DC, 2008.
10. Goffman, E. *The Presentation of Self in Everyday Life*. Doubleday (1959).
11. Goodwin, C. Professional Vision. *American Anthropologist 96,* 3 (1994), 606–633.
12. Honess, T. and Charman, E. *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*. Home Office On-Line Report, London, 1992.
13. Hong, J.I. and Landay, J.A. An Architecture for Privacy-Sensitive Ubiquitous Computing. In *Proc. MobiSys 2004*. ACM Press (2004), 177–189.
14. Hong, J.I., Ng, J.D., Lederer, S. and Landay, J.A. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. In *Proc DIS 2004*. ACM Press (2004), 91–100.
15. Iachello, G. *Privacy and Proportionality.* Doctoral Dissertation, Georgia Institute of Technology, Atlanta, GA, 2006.
16. Iachello, G. and Hong, J. End-User Privacy in Human-Computer Interaction. *Foundations and Trends® in Human–Computer Interaction 1,* 1 (2007).
17. Kahneman, D., Krueger, A.B., Schkade, D.A., Schwarz, N. and Stone, A.A. A Survey Method for Characterizing Daily Life Experience: The Day Reconstruction Method. *Science 306*, 5702 (2004), 1776–1780.
18. Langheinrich, M. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In *Proc. UbiComp 2001*, Springer (2001) 273–291.
19. Laudon, K.C. *Dossier Society: Value Choices in the Design of National lnformation Systems,* Columbia University Press, New York, 1986.
20. Lehikoinen, J.T., Lehikoinen, J., and Huuskonen, P. Understanding Privacy Regulation in Ubicomp Interactions. *Personal and Ubiquitous Computing 12*, 8 (2008), 543–553.
21. Linowes, D.F. *Privacy in America: Is Your Private Life in the Public Eye?* University of Illinois Press, Champaign, IL, 1989.
22. Lyon, D. *Surveillance Society: Monitoring Everyday Life*. Open University Press, Buckingham, UK, 2001.
23. Malhotra, N.K., Kim, S.S. and Agarwal, J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research 15*, 4 (2004), 336–355.
24. Massimi, M., Truong, K.N., Dearman, D. and Hayes, G.R. Understanding Recording Technologies in Everyday Life. *IEEE Pervasive Computing 9*, 3 (2010), 64–71.
25. Miller, A. Computers and Privacy. In *W.M. Hoffman and J.M. Moore (Eds.), Ethics and the Management of Computer Technology*. Oelgeschlager, Gunn, and Hain, Cambridge, MA (1982), 93–108.
26. Nguyen, D.H., Kobsa, A. and Hayes, G.R. An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies. In *Proc. Ubicomp 2008,* ACM Press (2008), 182–191.
27. Nguyen, D.H., Marcu, G., Hayes, G.R., Truong, K.N., Scott, J., Langheinrich, M. and Roduner, C. Encountering SenseCam: Personal Recording Technologies in Everyday Life. In *Proc. UbiComp 2009*, ACM Press (2009), 165–174.
28. Palen, L. and Dourish, P. Unpacking "Privacy" for a Networked World. In *Proc. CHI 2003*. ACM Press (2003), 129–136.
29. Privacy Protection Study Commission. *Personal Privacy in an lnformation Society: Report of the Privacy Protection Study Commission,* U.S. Government Printing Office, Washington, D.C., 1977.
30. Smith, H.J. *Managing Privacy: lnformation Technology and Organizational America,* University of North Carolina Press, Chapel Hill, NC, 1994.
31. Smith, H.J., Milberg, S.J. and Burke, S.J. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly 20*, 2 (1996), 167–196.
32. Stone, E.F., Gardner, D.G., Gueutal, H.G. and McClure, S. A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations, *Journal of Applied Psychology 68*, 3 (1983), 459–468.
33. Tolchinsky, P.D., McCuddy, M.K., Adams, J., Ganster, D.C., Woodman, R.W. and Fromkin, H.L. Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment, *Journal of Applied Psychology 66*, 3 (1981), 308–313.
34. Truong, K.N. and Hayes, G.R. Ubiquitous Computing for Capture and Access. *Foundations and Trends® in Human–Computer Interaction 2*, 2 (2009).
35. Westin, A.F. Social and Political Dimensions of Privacy. *Journal of Social Issues 59*, 2 (2003), 431–453.