Digital Neighborhood Watch: Investigating the Sharing of Camera Data Amongst Neighbors

A.J. Bernheim Brush, Jaeyeon Jung, Ratul Mahajan, Frank Martinez
Microsoft Research
One Microsoft Way, Redmond, WA 98052
{ajbrush, jjung, ratul, fmartin}@microsoft.com

ABSTRACT
In a neighborhood watch group, neighbors cooperate to prevent crime by sharing information and alerting police of suspicious activities. We propose a digital neighborhood watch (DNW) in which security cameras of individual homes work together to monitor the neighborhood. DNW could augment neighborhood watch by providing digital evidence of crime, increasing visibility of neighborhood activity, and automatically sending alerts when suspicious events occur. We investigate the appeal of sharing camera data with neighbors through semi-structured interviews with 11 households. Our participants validated the potential of sharing data with neighbors, particularly to provide evidence after an incident. But they also had security and privacy concerns about divulging their cameras' field of view and giving ongoing access to neighbors. For some participants, these concerns can be alleviated by enabling sharing of processed cameras views that include only the foreground activity or only public property (e.g., sidewalks).

Author Keywords
Sensing technology; neighborhood; privacy; security camera.

ACM Classification Keywords
H.5.1 Multimedia Information Systems.

INTRODUCTION
Neighborhood watches are groups of neighbors that cooperate to prevent crime (e.g., burglaries, vandalism) by watching neighborhood activity and alerting authorities when criminal activities are suspected. The U.S. National Sheriffs Association created a National Neighborhood Watch program in 1972 and many countries have similar programs. Rising crime in our own neighborhoods motivated us to investigate whether sharing data from sensors such as cameras and microphones across households could enhance neighborhood watch. At community meetings that we attended, law enforcement officers emphasized the need for residents to be the "eyes and ears" of the neighborhood and the power of sharing information among neighbors.

We envision a Digital Neighborhood Watch (DNW) system that is composed of sensors such as security cameras of individual households.[1] We investigate if such a system can augment neighborhood watch by: (1) providing digital evidence of incidents, (2) increasing visibility of neighborhood activity, and (3) automatically detecting and alerting for suspicious events (e.g., unfamiliar car drove by several times). DNW is in contrast to local authorities or governments installing and monitoring networks of cameras (e.g., CCTV cameras in England). Given the reluctance of many communities and authorities (including our own) towards such "big brother" technologies, we wanted to explore the feasibility of neighbors voluntarily sharing their own camera data with each other. Such sharing can enable inferences that data from individual homes cannot enable (e.g., a car cruising the neighborhood, without stopping at any home).

While the feasibility of DNW depends on several social, technical, and legal factors, in this paper, we focus on an important social factor—the value versus the privacy and security risks that households perceive with sharing camera data. Through semi-structured interviews we gather households' perspectives on sharing data for DNW with their neighbors, law enforcement, and security companies.

We find that DNW is a promising concept, but it entails challenges. Our participants were willing to share camera data with neighbors after an incident, which meets the goal of providing digital evidence. But the other two goals, increasing visibility and automatically detecting suspicious activities, are harder to meet because participants had concerns about divulging the location and field of view of cam-

CSCW '13, February 23–27, 2013, San Antonio, Texas, USA.

[1] Currently a wide range of home security systems from professionally installed and monitored systems to less expensive do-it-yourself systems are available. ABI Research estimates that in 2006, roughly twenty-six million systems were deployed in the U.S (~21% of households) and twenty-three million in Europe (~8% of households). It also predicts increased adoption as hardware becomes inexpensive. Of particular interest to us are the decreasing prices of cameras, making camera-based systems more affordable.

eras and giving ongoing access to neighbors. These concerns led us to propose and evaluate two processed camera views that only include the foreground activity and public property. We find that these views alleviate the concerns and encourage some participants to allow greater access for neighbors and police.

Our main contribution is uncovering what camera data people will share with neighbors for neighborhood safety and highlighting concerns that must be addressed to build a successful DNW system. Although our work focuses on sharing home security camera data, our findings about situations when neighbors would share and about data abstractions that remove sensitive parts of information can be applicable for other neighborhood-based sharing applications (e.g., water usage, coordinating electricity usage).

RELATED WORK

As usage of information and communication technologies (ICT) became more common, researchers studied the impact on local communities. Studying the wired suburb of "Netville" from 1997-1999, Hampton and Wellman found the community mailing list facilitated neighborhood-based interactions, led to knowing and chatting with more people in the neighborhood, and lowered barriers to collective action including organizing against the housing developer [9]. Kavanaugh et al.'s longitudinal survey of 100 households in the Blacksburg Electronic Village in 2001 and 2002 also showed that Internet use can strengthen community engagement and social contact [12].

Focusing on people working together to address crime in their neighborhoods, Lewis and Lewis analyzed a Chicago community crime forum [15]. Their study suggested crime prevention technologies should facilitate communication and discussions among residents. Our study of the potential for households to share data from their own security systems with neighbors meshes well with how the community crime forum was used. For example, forum members discussed sharing information and collecting evidence (e.g., writing down license plates numbers, wanting to observe property damage to cars overnight without staying up all night) both of which could potentially be supported by a digital neighborhood watch system.

Privacy concerns around video capture and recording, primarily in public spaces, have been studied by many researchers. For example, using the principles of Value Sensitive Design, Friedman et al. interviewed both people watching video from a university plaza (direct stakeholders) and those being watched (indirect stakeholders) [8]. They found participant's privacy judgments often included consideration based on physical harm, psychological wellbeing, and informed consent, and that more women expressed concern regardless of whether they were watching the video or being watched in the plaza.

Nguyen et al. [17] studied perceptions of pervasive video recording among indirect stakeholders for video recording encountered during their own lives (e.g., in restaurants and public places). Building on the Concern for Information Privacy (CFIP) model they asked participants about collection of data, improper access, unauthorized secondary use, and errors. Study results suggested ways to extend CFIP and indicated participants frequently assumed collection of video data when outside their home or private spaces in the U.S.A. These and other similar studies (e.g., of CCTV) provide valuable information about video-related privacy concerns, particularly among indirect stakeholders, for video captured in public or semi-public spaces. In contrast, our study focuses on household members, primarily as direct stakeholders, and their willingness to share video captured from personal security systems located at their homes to address neighborhood crime.

Related to our interest in cameras for security, Tullio et al. interviewed law enforcement personal including CCTV managers and police officers that use video from seven sites across the U.S. and U.K. [20]. Their findings included the value of human monitoring of CCTV to detect incidents and challenges around managing digital evidence (e.g., finding important parts of recordings). Our focus on individual households' complements Tullio et al.'s focus on law enforcement as well as other studies of CCTV.

One study that considered cameras in households was Beckman et al.'s study of 15 homeowners installing mock-sensors inside their homes for a home energy tutor application [1]. They recommended not using highly directional sensors such as cameras and microphones due to privacy concerns and installation errors where the mock sensors were not aimed to capture items of interest. Rather than studying cameras inside homes, we focus on external cameras for capturing spaces outside the home, having participants indicate to us which parts of their property they wanted to be captured by security cameras.

Finally, our study design, especially for privacy related questions, was inspired by previous work that presents principles and guidelines for designing privacy-sensitive systems [10, 13]—most notably the first stage of Iachello and Abowd's Proportionality Design Method assessing the legitimacy or appeal of an application [10]. We also share the general goal of understanding people's reactions to recording technologies in daily life with several projects (e.g., [8], [10], [16], and [17]), but our study is grounded in the context of DNW giving a unique focus on privacy and security concerns related to data sharing with neighbors.

STUDY METHOD

We conducted 11 semi-structured in-home interviews with 24 participants (13F, 11M) living in the northwest USA between Dec. 2011 and Feb. 2012. All but one home had at least 2 members over 14 years old. Households were compensated with a choice of software gratuity for each participant, up to four per household.

Given our interest in whether electronic sensor data could augment neighborhood watch activities we recruited only households that belonged to a block watch group or neigh-

borhood association. Beyond this requirement, we recruited households for diversity in terms of socioeconomic status, neighborhood crime rate, and experience with security systems. Our participants had a range of occupations including electrician, accountant, wine store owner, and retired. None were associated with our organization.

Five households (H7-H11) are in a neighborhood with a high crime rate relative to the region. For example, this neighborhood had 16 burglaries, 8 thefts, 5 arrests and 4 assaults from Jan. to Mar. 2012. The median household income in this neighborhood is $47,461, which is close to the national median ($49,445 in 2010). When asked about security concerns in the neighborhood, residents described frequent break-ins, hearing gunshots, and problems with drugs. These households were recruited through a neighborhood mailing list and personal requests by one of the authors who lives in this neighborhood. The author did not participate in interviews in his neighborhood so that the participants felt comfortable sharing their opinions about other neighbors. For consistency, he excluded himself from all interviews.

We recruited the other six households (H1-H6, interviewed first due to scheduling constraints) using a recruiting service. We worked with the service to locate eligible households by reaching out to police liaisons, block captains, and neighborhood associations. These six households were selected to be in different neighborhoods so we could interview people in different locations. We explicitly asked about neighborhood crime, and while we heard about occasional problems (e.g., mailbox theft, stolen cars left on the street), the level of incidents and the general concern was much lower than in the high-crime neighborhood.

Our goal in recruiting households with different levels of neighborhood crime was to explore how perspectives on sharing data might change with the level of recent crime. For instance, households in the high-crime neighborhood represent a population that might perceive considerable value in sharing sensed data with neighbors to prevent future crimes. If even these households have insurmountable security and privacy concerns, it seems unlikely that systems like DNW would be adopted in practice.

With regards to experience with security systems, six households (three in the high-crime neighborhood) have existing security systems, primarily door and window sensors, from different companies (e.g., ADT, Monitronics). Two of these six, both in the high-crime neighborhood, had experience with camera-based systems, either currently (H11) or recently (H9). This mix of participants allowed us to interview both people with the experience of living with security systems and people who could describe their ideal system without being biased by prior experience.

Interviews

We interviewed household members together. We began by asking about existing security precautions. Participants then indicated on aerial maps of their house and neighborhood where, if desired, they would place cameras. We asked about what features they would want in a security system, how they would want to access it, and whether they would tell their neighbors if they had the cameras.

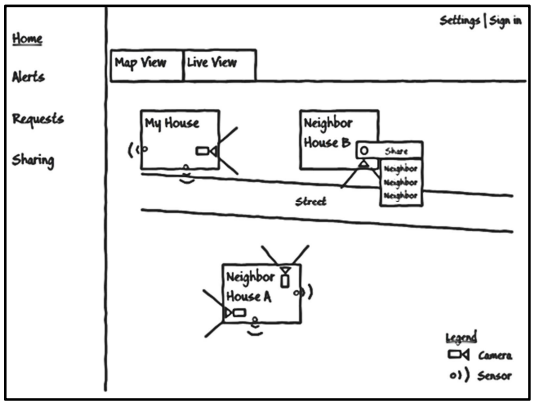
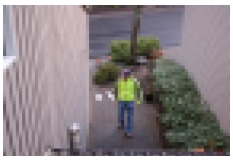


Figure 1. Digital Neighborhood Watch Paper Mockup

Next, we asked about their involvement in their neighborhood group and how frequently they interacted with their neighbors. We then asked about their willingness to share data from the cameras they had specified in the first part of the interview with neighbors. To ground this discussion we showed participants low-fidelity, paper mockups of a possible web interface for sharing (Fig. 1). These mockups were intended as probes to give participants some context and visuals to react to. In the interviews, we emphasized that we had not built a system and encouraged them to share their candid feedback and ideas. This effort was successful as the results will demonstrate that participants almost universally rejected the idea of sharing cameras feeds directly with neighbors that was illustrated in the mockups.

Lastly, we filled out a sharing chart through discussion with participants. The chart had rows describing groups they might share with: proximate neighbors (e.g., in view of cameras), other neighbors, law enforcement, and a security company that provided a service for detecting suspicious activity by analyzing information across multiple cameras. The chart had columns showing different types of data that could be shared (Fig. 2). Motivated by a desire to understand how data fidelity might affect sharing, we originally asked participants about sharing high fidelity data (2a), low resolution data (2b) and data that had been processed into textual descriptions of events (2e). Feedback described in the next section led us to add processed camera views showing only foreground activity (2c) or public property (2d) starting in the fifth interview.

For each row-column combination we asked participants if they would "Always", "Sometimes" (by request or under specific circumstances) or "Never" share. We used the sharing chart to stimulate discussion, allowed participants to rename groups as they desired, and prompted them to explain their choices.

Man in yellow shirt at door
Red car drove by
Two adults walked by
One person entered home

(a) High fidelity **(b) Low resolution** **(c) Foreground only** **(d) Public property only** **(e) Events**

Figure 2. Raw and processed camera data similar to those we asked participants about sharing with different groups of people. Starting with H5 Options (c) and (d) were added and Option (b) was discontinued, based on feedback from first 4 interviews.

Each interview lasted about two hours and was semi-structured as we discussed different relationships with neighbors, neighborhood groups, and law enforcement. We audio recorded and transcribed each interview. We then extracted over 700 items from interviews and field notes and analyzed the data using the affinity diagramming technique [2] based on a grounded theory approach. The authors collaborated on an iterative bottom-up affinity analysis of the items to derive key themes and findings.

A limitation of our study is that some of the participants' reactions could be speculative, given the difficulty of studying people's perceptions toward a new technology. We used interface mockups and image data from an existing surveillance camera to reduce this effect. Another limitation is that our study is based on a relatively small number of participants drawn from a few neighborhoods in the USA. Our findings, however, can form the basis for a broader survey.

RESULTS

A DNW system requires individual households to install camera systems. Perhaps not surprisingly given participants agreed to participate in an interview study about the use of cameras and sensing for home security, all our participant households except H8 were interested in having cameras that recorded videos outside their home. H8 felt their home was occupied most of the time and located such that criminals would be highly visible to others; however, they were open to cameras in the neighborhood to enable DNW.

More interesting to us, eighteen participants (at least one in each household) indicated they would be willing to participate in DNW by sharing some camera data. We discuss below the household sensing system features that appealed to households and challenges that affect the design of DNW.

Household Sensing Systems Desired

Participants wanted a median of 4 outdoor cameras per home. Typical placements included views of front yard, back door, and side yards. When asked about how long they would want to store the camera data, half wanted it retained less than a month (4 of those one week only). A computer at home and a T.V. were ranked as the most important places to view data from security cameras, but access on a mobile phone from outside the home was also highly ranked.

Participants described perceived security benefits including awareness, deterring crime, and for evidence. H11_M (M denotes speaker gender), currently using cameras, also highlighted non-security benefits such as watching themselves complete a major yard project ("it was cool because we built a really nice cedar fence and it [the camera] had documented that whole process") and watching animals ("I hung a bird feeder right in front of the camera one time just for kicks"). H3 also mentioned neighbors had shared video of a bear captured by their camera system. Not surprisingly, cost was a concern, but all ten households with interest in cameras indicated a willingness to pay.

We also asked participants if cameras should capture audio data. Somewhat surprising to us, 14 participants across 9 households wanted audio captured. Participants desiring audio described using it to detect specific sounds such as gunshots or glass breaking rather than to record voices (e.g., "The only reason I would consider audio would be for like a glass break sound" H9_M).

Two female participants, who did not want audio captured, explicitly mentioned not wanting to record conversations and one also felt audio would not offer much value saying "a crooked person would not be talking probably (H4_F)." We found it interesting that in four of the five households where participants disagreed on whether audio should be recorded, female participants did not want it recorded. This could be a similar effect for audio privacy that Friedman et al. [8] found for video with a much larger sample; women expressed more concern about video privacy regardless if they were watching the video or being watched.

Trust Not Proximity for Sharing Existence of Cameras

We asked households if they would inform their neighbors about installed cameras, a pre-requisite for sharing any sensed data. We initially thought participants might treat neighbors in the view of installed cameras (e.g., next door) differently. However, it quickly became clear that participants divided neighbors into groups based on trust, not proximity. Five households renamed the "proximate neighbors" group to "trusted neighbors" in the sharing chart.

While nine households said they would tell trusted neighbors they had installed cameras, they described several reasons for not telling other neighbors in the block watch, including those in view of the camera. For example, four households thought neighbors would think they were spy-

ing on them even if that was not intended.[2] Households in the high crime neighborhood told us they had been warned about certain houses by law enforcement. H10 specified that street-facing cameras must be disguised so untrusted neighbors would not realize that they were being observed.

When asked what they would expect from neighbors with cameras (when household members would be the indirect stakeholders being captured by neighbors), most households were consistent, not expecting neighbors to share presence or location of cameras with them. Four households preferred that other households tell them if they installed cameras, but had no expectations. H10_F said, "I wouldn't have any expectation that they would have an obligation to inform us anymore than we would have an obligation to inform them." Two households explicitly mentioned they had no expectation of privacy in public spaces.

Reluctance to Divulge Camera's Field of View

Participants described a reluctance to divulge a camera's field of view (FoV) even to people they would tell about the existence of cameras (e.g., "not your coverage, because you're opening yourself up" H3_M). The concern was security related—divulging the FoV leaks information about "blind spots" of the home security system. No household would consider sharing the camera's FoV with members of their neighborhood group and four would not share even if sharing is limited to trusted neighbors. Not being able to trust "friends of friends" and "kids of friends" was frequently mentioned as a reason to limit disclosure.

The parents in H2 went further and wanted to limit kids' knowledge of the FOV of some of the cameras ("H2_F "I would not want them [kids] to know exactly where they were") to deter sneaking out of the house. More generally, we asked the four households with children in them (H1, H2, H3, H6) about who in the household should have access to camera data. In all cases, the adults felt they would be the only ones with access to any recorded video, but kids should be able to see some of it live (e.g., in H2, they wanted images from a camera mounted at the front door visible on the TV so kids could check it).

Based on FOV concerns expressed in the first four interviews, starting with H5 we additionally asked participants about a foreground-only data sharing option (Fig. 2c), that shares the camera data without divulging the FoV. Three households, all in the high crime neighborhood, indicated they would share this processed data with more groups including other neighbors and police than high-fidelity data (Fig. 2a). (H11_F "we want to tell that we have a camera, we just don't want to tell them where it is. And this way we could show them the guy in the yellow shirt, but they wouldn't know [the FoV]").

Will Share Evidence with Good Reason

One potential benefit of DNW is providing digital evidence of incidents. All ten households with interest in installing cameras indicated that they would sometimes be willing to provide data from their cameras as evidence. However, some participants stressed the need for a good reason for the request ("it really depends on the context on what they're asking for" H9_M) and that the severity of the incident would influence willingness to share ("if it was a murder, whether I didn't like you or not, I'd probably still share that information" H10_M).

While people had concerns about neighbors, five of the six households that we asked explicitly were willing to share existence and cameras' FoV with law enforcement, and all except H5 were willing to share high-fidelity video on request. In fact, H4_M said he would provide evidentiary data directly to law enforcement, rather than to neighbors ("I feel more comfortable sharing the images with the police department because they're the ones who need to take the action.") Again, certain participants stressed the need for a valid reason before they would share data.

We initially asked about sharing low-resolution data (Fig. 2b) as blurred video could reduce privacy risks while not compromising situational awareness [3]. However, starting with H5, we stopped asking about it; all earlier households felt that if they were going to share they would share high-fidelity data ("why would anybody have low resolution, what's the point?" H4_M).

Limited Willingness to Share Direct Access to Cameras

A DNW system could provide greater visibility into neighborhood activity by sharing ongoing access to cameras. For instance, a person could access a neighbor's camera to view parts of the neighborhood that are not visible in her own cameras. However, households were universally reluctant to provide direct, ongoing access to their cameras to neighbors, even trusted ones (e.g., "if an incident happened we'd be willing to share, but I don't think I would want anybody to have free access" H2_M). In a few special cases, participants would share access. Three households were willing to provide access to their cameras while they were on vacation, one when teenage children were home alone, and two would trade access with neighbors that also have cameras.

Given the reluctance to grant access, starting with H5, we asked about sharing processed data that only contained public property (Fig. 2d) such as sidewalks and parks. Three households were willing to "Always" share this data (from certain cameras) with trusted neighbors and law enforcement. H10 and H11 were also willing to provide this data to other neighbors in their neighborhood group.

When asked, four households were positive about adding cameras to public spaces, suggesting problem spots like parks. However, in general, participants were more con-

[2] While laws in the USA vary by city and state, to the best of our knowledge it is generally legal to point cameras and record videos of streets and outside parts (e.g., yards) of others' homes. In such places, there is no reasonable expectation of privacy [11]. Recording videos of inside parts or recording audio is not legal without consent. EU directive 95/46 appear more restrictive than laws in the USA, but its implementation by member states varies [4].

cerned about these cameras than household systems, wanting to avoid "turning into what England has" (H5_M), and questioning who should be able to access them (e.g., all neighbors). The primary concern was privacy—participants felt that being digitally watched by anyone in the neighborhood (without their knowledge) was worse than someone visible watching from the street.

Cautious Interest in Suspicious Activity Detection

Several of the suspicious activities that police detectives recommend watching for (e.g., an unknown car driving by several times) would be easier to detect by comparing data from multiple households. So, we asked participants about what fidelity of data, if any, they would contribute to a service that could potentially detect some of these activities using computer vision techniques [e.g., 19].

Some participants had a positive response to the idea of using data from multiple households. H9_F described how data from several neighbors' cameras had been combined to catch someone following a UPS truck and stealing packages saying "they got a face of her off of one house and they got her license plate because she parked her car next door from the house." H10_F compared suspicious activity detection to the community policing program, saying "a little bit like what Eyes on the Street [is] doing right now."

Five households, four in the high crime neighborhood, indicated they would share events (Fig. 2e) with a detection service on an ongoing basis; the other five with interest in a household sensing system were willing to do so only sometimes. Seven households were willing to share high-fidelity data upon specific requests with a suspicious activity detection service (e.g., if police were looking for a specific car).

However, participants also raised concerns about suspicious activity detection including who would run the service, data retention policies, and bandwidth requirements. Three households strongly preferred that a detection service run on their own computers and exchange data peer-to-peer rather than sending to a third-party service. Another major concern was incorrect or overwhelming notifications. Seven households, including all six with existing security systems, expressed concerns about false alerts from an automatic system. Two had modified their existing systems due to frequent occurrences of falsely detected motion.

DISCUSSION

Neighborhood Types vs. Acceptability of DNW

When planning the study we hypothesized that level of crime in a neighborhood could impact how much benefit households perceived in sharing their security data with neighbors and their willingness to do so at all. We were surprised by the broad similarity in attitudes we found in high and low crime neighborhoods. Households were equally willing to share data for evidence, and interest in sensing audio was present in both types of households.

As described earlier, we did observe two differences, however. First, households in the high crime neighborhood indicated a greater willingness to share events with a detection service on an ongoing basis (4 of the 5 households from the high crime neighborhood were interested). Second, due to untrusted or even known-to-be dangerous neighbors, participants in high crime neighborhoods emphasized the importance of hidden cameras to limit possible reprisals against them from collecting and sharing camera data. However, households in the low crime neighborhoods also had concerns about who they would share with and about leaking the camera's FOV (and thus blind spots).

Although we did not investigate them in this study, other attributes of a neighborhood may impact the acceptability of DNW, including household structure (e.g., apartment buildings vs. single family houses), cultural norms, and residents' lifestyle (e.g., urban vs. rural). We leave the study of these attributes as avenues to explore next.

Complex Neighborhood Trust

We began our study with a belief that participants might treat proximate neighbors differently and might treat all other neighbors in the block watch equally (e.g., choosing to share or not). As we described, participants quickly made clear to us that their trust and relationship with the neighbors was more important than proximity and had reasons they might not share the presence of cameras with members of the block watch. This suggests to us that, when designing a DNW system, allowing neighbors to construct their own ad-hoc sharing groups might be a more viable approach than having a "block watch" group. However, the challenge of facilitating broader sharing still remains as DNW likely becomes more effective as the number of participating households increases.

The increasing mobility of people can further complicate neighborhood trust relationships. In our study, participants showed heightened concerns over sharing camera data with renters in the neighborhood. One interesting issue to examine is to understand existing practices people use to develop trust with their neighbors and to find ways to help them grow their trust network with technical assistance. For instance, when a new neighbor moves in, there should be ways for newcomers to easily discover existing DNW groups and to introduce themselves to interesting groups. Neighborhood social networking sites such as Nextdoor.com may be a useful way to bootstrap a trusted community for DNW.

Sharing Security Camera Data vs. Other Data Types

Participant's concerns about divulging their cameras' FOV highlights a key difference compared from findings of studies of sharing other types of context, particularly mobile context such as location [e.g., 5, 14]. The placement and FOV of household cameras are highly sensitive and even a single disclosure could leak information about blind spots of a home security system. In contrast, sharing your current location might be considered less sensitive and its sensitivity potentially reduces with time, allowing participants to make different decisions about sharing with the same person at different times without long term consequences.

The importance our participants placed on knowing "why" people would be requesting their camera data was also found to be an important decision factor for sharing location in Consolvo et al. [5]. However, in contrast to this study and the findings of Lederer et al. [14], which showed that "who" was requesting the information was the most important factor, for our participants, "why" data was needed seemed to be at least equally important and sometimes more important than "who" was asking. One reason for this may be that the stakes are higher if camera data is misused (e.g., accidental leakage of personal moments, repurposed as video evidence in court). Another reason could be that we asked about sharing with very different groups (e.g., neighbors, law enforcement) than those typically studied in context sharing (e.g., family, friends, co-workers).

Implications for Other Neighborhood Sharing Systems

We focused on whether and how participants might share camera data with neighbors for security reasons; other examples of sensing applications that require data sharing amongst neighbors include coordinating electricity usage to reduce peak load on local transformers, comparing neighbors water usage (e.g., [7]), or sharing commute patterns to identify carpooling opportunities. Our findings suggest interesting ways to reconsider sharing of other types of data with neighbors.

First, systems for sharing sensed data (e.g., water usage, electricity) often collect data from large numbers of households and then share back anonymized data. However, our participants were generally more receptive to sharing data based on specific events (e.g., police looking for a specific car) than sharing ongoing information. Considering ways that neighbors can be alerted to situations and asked to respond to specific actions rather than sharing ongoing data may be fruitful. For example, for reducing peak load on transformers, alerting households to high loads and incenting them to reduce usage at that moment might be a viable alternative to collecting data for neighbors and trying to coordinate usage. Similarly, we can look for spikes in water usage at the neighborhood level and alert households to those events.

For DNW, we also found that abstractions of the data that preserved appropriate levels of privacy (e.g., foreground only or public-property views) tended to increase the willingness of some participants to share. Exploring whether similar abstractions exist for other types of data, particularly for situations when fully anonymous data is either not possible or less useful, is an interesting research opportunity. For example, neighborhood water saving competitions might be more successful if neighbors know who they are competing against, but households may be more willing to participate if they can share data at a level of abstraction that prevents neighbors from seeing specifics (e.g., showing a comparison outcome of which neighbor had higher usage instead of total daily usage which could leak when people are on vacation).

While these may or may not be good ideas in a given context, we believe our findings suggest alternatives for other researchers working on neighborhood data sharing systems to consider as they pursue their specific scenarios.

CONCLUDING REMARKS

Our findings make us cautiously optimistic about the feasibility of DNW. All but one of our households, including those outside the high crime neighborhood, saw advantages in deploying a camera-based security system. All households were willing to participate in DNW to provide digital evidence. Interest in sharing data to support awareness and detect suspicious activity was limited, however, due to security and privacy concerns. But we were encouraged by the interest in activity detection from households in the high crime neighborhood and comparisons to community policing. Further, the options of sharing processed camera data, with only foreground and public-property, helped address concerns for some households.

Informed by our study, we are building on top of HomeOS [6] an easily-installable, low-cost home camera system that incorporates features to support the types of sharing towards which our households indicated they were open. For example, we are making it easy to archive and share sections of recorded video to allow households to provide evidence when needed as well as share foreground-only and public-property camera views to support sharing without fully divulging the location and field of view of their cameras. Incorporating mechanisms that allow people to share more or less data will be necessary to allow ongoing negotiation through a DNW system as situations change [18]. We are also investigating advances in computer vision, including techniques to track objects over obfuscated videos [21], which may enable an effective DNW system that respects people's privacy and security concerns.

During our research, our own neighborhoods have continued to experience crimes including daytime burglaries and gun incidents. These events continually renew our motivation to explore ways in which technology can help reduce crime while being sensitive to the privacy and security concerns of household members. We are aware that a DNW system, like CCTV, can be abused (e.g., to spy on neighbors). While our participants felt that neighbors' cameras did not alter their expectation of privacy, we plan to revisit this issue as we deploy prototypes.

REFERENCES

1. Beckmann, C., Consolvo, S., LaMarca, A. Some Assembly Required: Supporting End-User Sensor Installation in Domestic Ubiquitous Computing Environments. UbiComp 2004, 107-124.
2. Beyer, H., Holtzblatt, K. Contextual Design: Defining Customer-Centered Systems. Morgan Kaufmann, 1998.
3. Boyle, M., Edwards, C., and Greenberg, S. 2000. The effects of filtered video on awareness and privacy. CSCW 2000, 1-10.

4. British Institute of Internal and Comparative Law, The implementation of Directive 95/46/EC to the Processing of Sound and Image Data, 2003.
5. Consolvo, S., Smith, T., LaMarca, A. Tabert, J., Powledge, P., Location Disclosure to Social Relations: Why, When & What People Want to Share. CHI 2005, 81-90.
6. Dixon, C., Mahajan, R., Agarwal, S., Brush, A., Lee, B., Saroiu, S., Bahl, P., An Operating System for the Home. NSDI'12, 337–352.
7. Erickson, T., Podlaseck, M., Sahu, S., Dai, J., Chao, T., Naphade, M., The Dubuque Water Portal: Evaluation of the Uptake, Use and Impact of Residential Water Consumption Feedback. CHI 2012, 675-684.
8. Friedman, B., Kahn, P, Hagman, J., Severson, R., The Watcher and the Watched: Social Judgments About Privacy in a Public Place. Human-Computer Interaction, vol. 21, 2006, 235-272.
9. Hampton, K., & Wellman, B., Neighboring in Netville: How the Internet Supports Community and Social Capital in a Wired Suburb. City & Community vol. 2, no. 3 2003, 277-311.
10. Iachello, G., & Abowd, G.D. Privacy and proportionality: adapting legal evaluation techniques to inform design in ubiquitous computing. CHI 2005, 91–100.
11. Katz v. United States. 389 U.S. 347;88 S. Ct. 507 (1967)
12. Kavanaugh, A., Carroll, J., Rosson, M., Zin, T., Reese, D., Community Networks: Where Offline Communities Meet Online. Journal of Computer-Mediated Communication, 10(4), article 3.
13. Langheinrich, M. Privacy by design-Principles of privacy-aware ubiquitous systems. UbiComp 2001, 273–291.
14. Lederer, S., Mankoff J., Dey, A.K., "Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing". CHI Extended Abstracts 2003, 724-5.
15. Lewis S., and Lewis, D., Examining Technology that Supports Community Policing. CHI 2012, 1371-1380.
16. Massimi, M. et al. (2010). Understanding recording technologies in everyday life. IEEE Pervasive Computing, 9(3), 64–71.
17. Nguyen, D., Bedford, A., Bretana, A., Hayes, G., Situating the Concern for Information Privacy through an Empirical Study of Responses to Video Recording. CHI 2011, 3207-3216.
18. Palen, L., & Dourish, P. Unpacking "Privacy" for a Networked World. CHI 2003, 129–136.
19. Song B., Ding C., Kamal A. T., Farrel J. A., Roy-Chowdhury A. K., Distributed Camera Networks. IEEE Signal Processing, vol. 28, issue. 3 May 2011, 20-31.
20. Tullio, J., Huang, E., Wheatley, D., Zhang, H., Guerrero, C. Tamdoo, A., Experience, Adjustment, and Engagement: The Role of Video in Law Enforcement. CHI 2010, 1505 – 1514.
21. Upmanyu M., Namboodiri A. M., Srinathan K., Jawahar C. V., Efficient Privacy Preserving Video Surveillance. ICCV 2009, 1639-1646.