Participatory Privacy in Urban Sensing

Katie Shilton, Jeff Burke, Deborah Estrin, Mark Hansen, and Mani B. Srivastava

***Abstract*— Urban sensing systems that use mobile phones enable individuals and communities to collect and share data with unprecedented speed, accuracy and granularity. But employing mobile handsets as sensor nodes poses new challenges for privacy, data security, and ethics. To address these challenges, CENS is developing design principles based upon understanding privacy regulation as a participatory process. This paper briefly reviews related literature and introduces the concept of *participatory privacy regulation*. *PPR* reframes negotiations of social context as an important part of participation in sensing-supported research. It engages participants in ethical decision-making and the meaningful negotiation of personal boundaries and identities. We use PPR to establish a set of design principles based on our application drivers.**

***Index Terms*— Urban sensing, privacy, ethics, participatory design, participatory research**

I. Introduction

Networks of mobile phones, familiar tools carried by billions, create a substrate that can support widespread public participation in data collection and dissemination. In *participatory urban sensing*, everyday mobile phones become a platform for coordinated investigation of the environment and human activity [1-5]. The UCLA Center for Embedded Networked Sensing's (CENS) urban sensing group is initiating projects to introduce these technologies into the public realm. This anticipates sensing being used by the general public; suggests new possibilities for understanding social, political or, more generally, "urban" processes; and elicits new requirements for design and network infrastructure.

While embedded wireless sensing already provides scientists and engineers unique insights into the physical and biological processes of the natural and built environments, sensing *by* the public through the organized use of mobile technology presents significant technical and ethical challenges. Never before has sensing been so close to individuals, and so intermixed in their daily lives. Never before has the public had such ability to use familiar tools to collect, control, and share data. The ramifications of granular, personal and easily shared information demand leadership by designers of these systems to proactively integrate the needs, requests and potentially diverse values of system users. To build socially trusted systems, we believe that the intended users must be significantly involved in the design process.

Motivating and operationalizing user participation within the fast-paced research and development activities of participatory urban sensing is challenging, important, and very broad. This paper suggests one approach to incorporating participation: using a participatory model to answer privacy dilemmas presented by urban sensing systems. Privacy is one of the first ethical challenges raised by users of systems that track location or automatically capture images, and serious privacy concerns have already surfaced in CENS pilots. This paper briefly reviews related privacy literature and introduces design principles based upon *participatory privacy regulation*: a flexible approach to privacy that incorporates both group and individual decision-making about disclosure boundaries to negotiate trust and commitment between participants and urban sensing systems.

CENS urban sensing projects focus on enabling campaigns—organized efforts for data collection and analysis. For example, the Personal Environmental Impact Report (PEIR) uses geo-temporal data gathered with mobile phones to assess personal environmental impact [6]. PEIR participants volunteer to carry mobile phones and GPS devices as they go about their daily routines (Fig. 1).

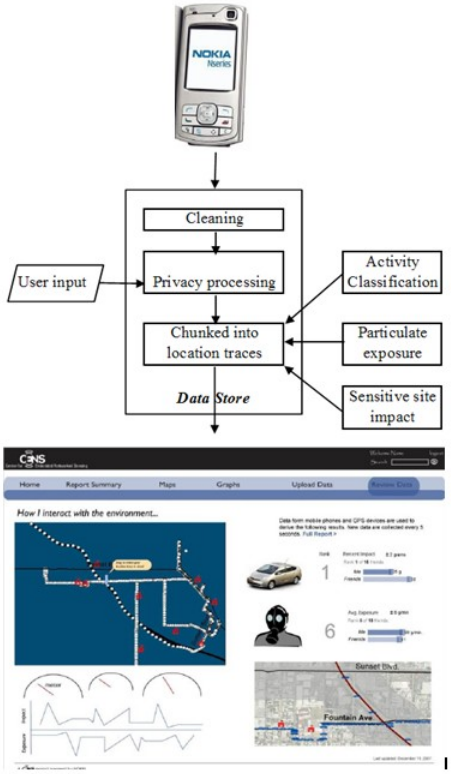

Figure 1: PEIR documents and shares user movements

Manuscript received April 9, 2008. This work is supported in part by the National Science Foundation and Nokia.

All authors are with the Center for Embedded Networked Sensing (CENS), University of California, Los Angeles, 3563 Boelter Hall, Los Angeles, CA 90095-1596 (corresponding author Katie Shilton: +1 310.825.3239; e-mail: kshilton@ucla.edu).

The phone records latitude and longitude every few seconds and uploads that data to a central database. Processing this data allows the PEIR system to infer a participant's activities, such as walking, driving, taking a bus, or staying indoors. The system combines these activity inferences with models of exposure to air pollutants and data about emissions and carbon footprint of the participant's activities. The system then presents daily location traces as well as estimated emissions of impact and particulate matter exposure to the participant through a personal web interface. Participants can also share their aggregate impact and exposure using social networking sites such as Facebook.

CENS is also developing systems for participants to gather and share data about neighborhood walkability and community assets. Participants use these systems to collect and organize geotagged and annotated photographs of their neighborhood. Future work in environmental and health applications may include automatically captured images, sound, or biometrics.

II. Background

Our evolving approach to the design of sensing systems has roots in participatory research (PR), participatory design (PD) and ubiquitous computing literatures. PR's success bridging gaps between research and practice [7] and its potential to empower participant decision-making [8] are uniquely suited to designing and managing systems embedded in people's everyday lives. In addition, participatory *design* methods can help systems accommodate the fluidity of people's willingness to collect and share data about themselves [9]. Because ubiquitous, networked sensors enable data collection in all spaces and places of their users' lives, they imply continuous *participation* of people either *in* or *with* the system. People can be involved *in* the system simply by agreeing to collect data. Such activity would be fairly passive from the standpoint of participatory research ethics [8]. In order to build systems that collect both meaningful and ethical data, the system must encourage people to engage *with* it. This means that participants are included in decisions about system design and use [8]. Empowering participants to make decisions about data collection, analysis, and research results preserves the autonomy of individuals interacting with otherwise invasive capture technologies. Pursuing participatory research may also lead to better research outcomes [7, 10]. For instance, involving users in research design can help systems designers recognize and meet the needs of populations underrepresented among researchers. Engaging communities in research can incorporate *local knowledge* into the research process, knowledge that is held by community members and developed through experience living within that time and place [10]. This process generates a unique set of technical and policy requirements for participatory urban sensing.

Participation itself is not the only relevant challenge in urban sensing. Privacy regulation and privacy protection are critical topics in the design of ubiquitous and pervasive systems [11-15]. Technical approaches to privacy design include: privacy warning, notification, or feedback systems [13, 16, 17]; methods for identifying privacy vulnerability in information systems [18]; systems that enable user choices about data sharing [12]; identity management systems [19]; and selective retention systems [13]. Other technical approaches to protecting user data include encryption, privacy-enhancing technologies (PETs), and statistical anonymization of data [20, 21]. Additional previous work explores data retention or its opposite, systematic 'forgetting' [22, 23]. Technical approaches to data privacy have also emerged in e-commerce [24, 25], data mining [26, 27], human-computer interface and interaction [28, 29], security [30], social networks [31], and mobile and sensor networks [32-35]. Despite this cross-disciplinary attention, *building systems* that protect user privacy remains a challenge. In a survey of technical approaches to privacy in human-computer interaction, Iachello and Hong [29] outline unaddressed "grand challenges" for meaningful privacy design, including: (a) developing standard privacy-enhancing interaction techniques; (b) developing analysis tools to evaluate privacy design principles; and (c) understanding the relationship between user concerns and technology acceptance.

Also relevant to participatory sensing is literature on the ways in which individuals respond to privacy issues. Individuals regulate the information they share about themselves according to personal and social variables. Such regulation can be a process of enforcing personal boundaries (including measures taken for safety, or to protect seclusion) or a method of portraying particular identities (such as boss, spouse, or student) [28]. Convention and environment shape the desire for protecting information about oneself [20, 36]. The customs of a society, place, or space have ongoing influence on these personal decisions. Scholars such as Nissenbaum [37] suggest that individuals' sense of appropriate disclosure, as well as understanding of information flow developed by experience within a space, contribute to individual discretion. For example, whispered conversations in crowded cafés may feel private, because there are no known modes of distribution for that information [36]. Individuals may also be willing to disclose highly personal information on social networking sites because they believe they understand the information flow of those sites [38].

The value of maintaining such fluid decision-making is debated within philosophical, sociological, legal, economic, and computing literature. Recent work by the National Research Council [20] brings together viewpoints from many of these fields, suggesting that privacy retains social importance and value, even withstanding computing technologies predicated on capture and governments increasingly focused on information "awareness." As well, experimental work [39] and public surveys [40, 41] suggest popular concern about exposure of personal information.

Nissenbaum [37] labels this concern for fluid and variable disclosure "contextual privacy" and argues that its absence not only leads to exposure, but also decreasing individual autonomy and freedom, damage to human relationships, and eventually, degradation of democracy. Other researchers similarly suggest that concerns about data capture extend beyond the protection of individuals. Curry, Phillips and Regan [42] write that data capture makes places and

populations increasingly visible or *legible*. Increasing knowledge about the actions of people and their movements through space has historically led to a type of function creep around data reuse—the analysis of amassed personal data for unintended, largely commercial applications. Function creep around secondary data uses enables social discrimination through practices such as price gouging or delivering unequal services predicated upon demographic data.

III. Defining Participatory Privacy Regulation

If decisions about information sharing and protection are context-dependent and variable, how can urban sensing systems respect such variability? CENS systems currently employ mobile phones as sensors. The systems must therefore meet the challenge of data collection carried out in public, personal, and liminal spaces. This is distinct from data collection systems installed in fixed locations such as homes or workplaces [13, 19, 43].

We recognize the importance of balancing the invasive qualities of these systems with their value for participants. To address this balance, CENS has established design principles based upon the concept of privacy regulation as a *participatory process*. Privacy regulation as *participatory* means that decisions about personal disclosure boundaries are part of engagement in research or system design. Such involvement can range from passive to fully self-mobilized, with the degree of participation dependent upon the roles and activities in which a person is involved [8]. Privacy regulation as a *process* means that decisions to withhold or disclose information are more complicated than can be addressed by an on/off switch or pre-set system settings. People control access to the self [28, 44], or access to information about the self [20] according to context. Such decisions are intimately tied to the identity a person assumes (e.g. parent, boss, friend) and the people and places with which she interacts [28]. Privacy therefore acquires specific, variable, and highly individual meaning in specific circumstances and settings [39, 44, 45]. We argue that urban sensing systems must allow people to negotiate social sharing and discretion much as they do in non-instrumented settings.

In addition to occurring in many places and spaces, negotiations of privacy occur in all phases of research. Control over capture is part of defining data collection requirements. Decisions about data resolution are part of presenting project results. Data sharing and retention are implicated in decisions about research outputs and goals. The process of negotiating privacy is indelibly a part of research. (We have situated privacy processes within participation in Figure 2.) Participation in the entire sensing process can help users understand a system's information flow, weigh the costs and benefits of sharing information, and make informed, context-specific decisions to disclose or withhold data.

Participatory privacy regulation therefore stems from dual requirements: giving participants control over data gathering and sharing according to their context and preferences; and giving participants a meaningful role in the research process. Participatory privacy regulation entails providing both groups and individuals choices about sharing and discretion throughout urban sensing system design and use. Because privacy issues arise even in pilot urban sensing projects, we believe that participatory privacy regulation should be considered from the very beginning of the design process.

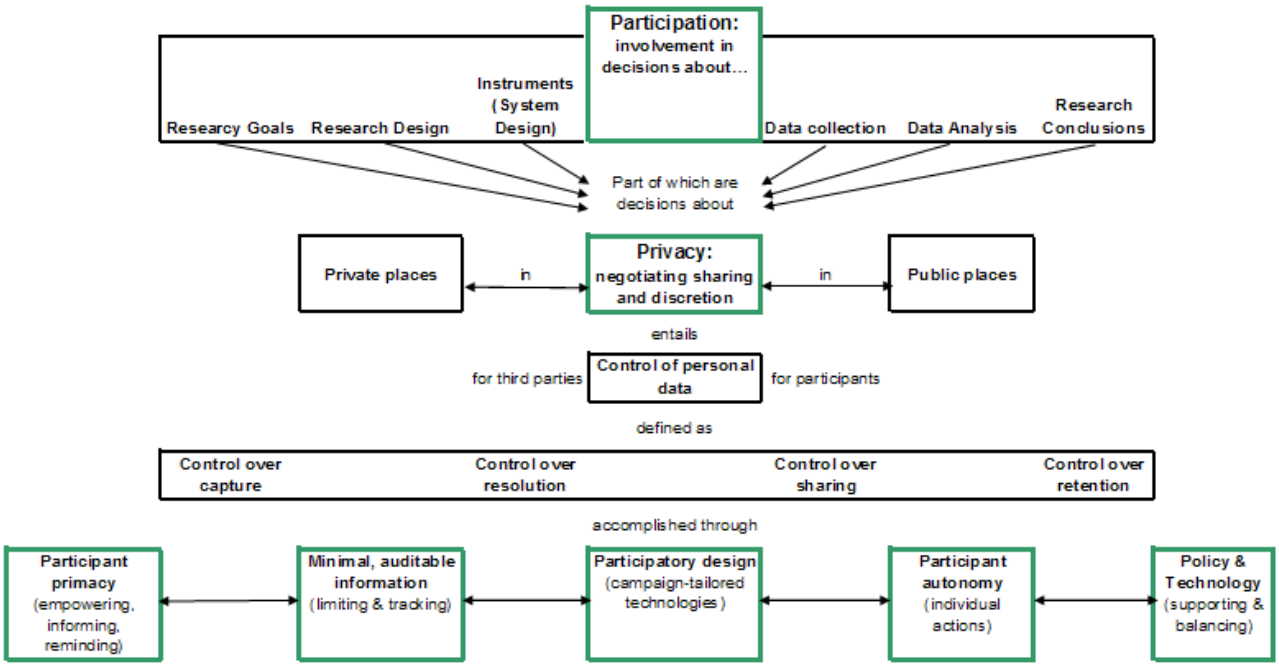

Figure 2: Privacy as part of participation

IV. Design for Participatory Privacy Regulation

Drawing on examples from the PEIR project, we have developed five broad principles to guide our design process. By considering privacy decision-making throughout participatory sensing projects, these principles incorporate disclosure decisions as part of participants' commitment to a project. We suggest current and emerging software developments guided by each design principle to help urban sensing systems facilitate participatory privacy regulation. Further development of new sensing applications and cooperation with participants will illuminate ways in which we can adapt and extend these principles.

A. Participant primacy

The mobile handset users, whose everyday devices become sensors in coordinated campaigns, should be primary participants in urban sensing projects, taking on the role—and responsibilities—of researchers. Because sharing and discretion decisions can occur throughout the process of research design, instrument design, and analysis, participatory privacy regulation is most meaningful and effective when participants are recognized as co-researchers. Design principles for participatory privacy regulation must therefore encourage cooperative control between system designers (often students and staff), community or domain research leaders (individuals who instigate and lead campaigns), and research participants (individuals who collect data).

Positioning participants as researchers requires that participants understand how the system collects, represents, and processes their data. A critical piece of this understanding is perception of the risks and benefits of disclosure and discretion. Envisioning negotiation of capture and sharing as critical to the research process will encourage participants to exercise control of their data and engage with disclosure decisions. Participant researchers may also better understand tensions between research needs and participant preferences, such as possible trade-offs between data accuracy, granularity and privacy. Designers must face the challenge of helping participants who lack the technical vocabulary or experience with data to understand these processes.

User interface: For participants to act effectively on their research responsibilities, software and user interfaces should make it easy to understand benefits and consequences of data capture and sharing throughout the data life cycle. Informing and educating participants about their data will be a critical component of participatory sensing system design. Visualizations to help participants understand their data, such as interfaces to allow individuals to browse their geo-temporal trace, can help participants identify data they deem too sensitive to share. Challenges for designers include not only developing novel interfaces that are legible to participants, but doing so early in the pilot process. An additional challenge discussed in more detail below is developing methods for incorporating participants in the interface design process.

***Encouraging responsibility*:** Project leaders and designers can use system software to promote responsible data practices. For example, evaluations of participants' contribution might include metrics representing how little third-party data a participant shares. Such metrics would encourage participants to avoid capture of third party data; to aggregate captured third-party data to make it less revealing; or to delete such data from the system entirely. System alerts or reminders that prompt participants to create data retention or reuse policies can also encourage conscientious data management as part of research responsibilities. The participatory sensing registration process should additionally inform potential participants about their responsibilities for data management, including legal ramifications of irresponsible data collection such as voyeurism [46] or eavesdropping [47]. Developing effective alert mechanisms that do not disrupt data collection or annoy participants is a considerable design challenge.

Flexible participant identities: Urban sensing software should support flexible participant identities to allow participants to adopt diverse research roles. Participants may wish to mask their identity, or refuse to share it at all. We are exploring the development of authentication process that support strong identity as well as anonymous, pseudonymous, and confidential identities.

B. Minimal and auditable information

Essential to building participatory approaches to privacy within urban sensing systems is capturing data that is relevant to specified research objectives while minimizing the capture of peripheral information. Parsimonious capture targets the data needed for research and new knowledge creation, but limits the possibilities for the invasion of participant privacy through retention of nonessential personal data. Minimizing capture also creates a discrete, understandable data set, helping participants comprehend and consent to sensing campaigns.

***Control over capture*:** Because participants are likely to have different data collection preferences and disclosure thresholds, sensing software must allow for both coarse- and fine-grained protection. Sensing software can provide simple, coarse-grained support for flexible privacy decisions by allowing participants to turn the mobile phone sensing software on and off. To address the challenge of more fine-grained control over data capture, systems could incorporate techniques such as buffered capture into appropriate campaigns. Buffered capture is a method by which data is captured for short periods, but discarded unless the participant takes explicit action [13]. Because participants must explicitly take action to retain data, buffered capture gives participants granular control over data collection. This fine-grained adjustment can help users avoid capture of irrelevant or compromising data, but challenges us to design systems which both support and benefit from minimal data collection.

Audit mechanisms: A strong authentication process and encrypted data storage are necessary to ensure that only individuals can access their personal data stores. Secure storage must also support the various processing, sharing, reuse and retention functions discussed below. Urban sensing systems should also audit data to ensure compliance with participant-specified access policies, data retention dates, and reuse policies. In keeping with the principle of participant

primacy, a challenge will be building auditing mechanisms to be viewable, legible, and useable by participants.

C. Participatory design

Participatory design is a practice that incorporates users as co-designers of a system [9, 48, 49]. CENS designs sensing systems as research instruments. Technology development is therefore part of a broader process of defining research methods and goals. Decisions about how to collect, represent, and share data affect design and implementation of sensing tools. Urban sensing systems must respond to users' planning, implementation, and evaluation processes.

Design in partnership with user groups is integral to participatory privacy regulation. A group design process can facilitate discussion and decision-making about campaign-specific privacy requirements. There is evidence that privacy decision-making is often difficult for individuals. In particular, people have trouble determining the future costs of relinquishing present privacy [20, 31]. Though participants should be able to make data collection, sharing, and retention choices to reflect their own boundaries and identities, the burden of this decision-making rests heavily on individuals. To mitigate some of this burden, designers and project leaders should encourage group discussion of data needs and disclosure risks. Communities can use immersion in the design process to identify concerns that individuals may miss. Participants and designers can then decide whether default system settings should be more or less oriented towards disclosure and sharing to mitigate pressure on individual in-situ decisions. In cases where especially sensitive data is collected (e.g. biometrics or personally identifying information), the project team may consider defaulting towards less sharing and greater data security. Group discussion will also illuminate places and times in the data life cycle when a research community may choose to take certain disclosure precautions or, alternatively, enable sharing. A participatory group process will provide design guidelines to tailor software for individual projects. For example:

***Aggregating data*:** Following the principle of minimal information, participant groups may decide to aggregate and share geo-temporal data only at the neighborhood level, rather than identify individual homes or workplaces. Alternatively, research groups may opt to record granular data, but share only derivative metrics to protect sensitive raw data. In PEIR, for instance, the system allows participants to share derivative measures of their total emissions or exposure rather than sharing their location traces. Urban sensing software must be able to adjust capture, storage, and representation of location traces to incorporate such decisions into system default settings. An additional challenge is that such flexibility must often be incorporated early in the design process, as the approval (by institutional bodies such as university Institutional Review Boards) and acceptance (by participants) of real-world pilots can depend upon such aggregation.

Selective sharing: Research groups may also want to dictate how, and with whom, participants share their data. Groups may opt for selective sharing of data by limiting distribution to the research group, or perhaps to only a few designated individuals. This challenges authentication processes and user permission descriptors to be flexible enough to allow for campaign-specific definitions of data access.

Tailoring capture: Research groups may also set minimal information capture policies, including deciding what data will be sensed and recorded (e.g. location, image, or other data), when and where data capture is encouraged (discrete vs. continuous, public vs. private spaces), and how visible the capture devices should be when participants record data in public (notification of third parties vs. confidentiality). Research groups should also dictate what personally-identifiable information is collected and stored about their participants, depending on their research needs and the sensitivity of the project. These challenges affect design of the mobile phone sensors. Software such as Campaignr [50] that runs on mobile phones should support tailored capture.

Customizing retention and reuse: Urban sensing systems may also need to adapt to research group policy about retention and reuse. A research group may decide to retain data indefinitely for future analysis, or dispose of data immediately after analysis. Because research group policy may dictate default retention metadata assigned to their dataset, designers must be particularly careful with pilot data, for which group preferences and parameters may not be known.

D. Participant autonomy

Participant autonomy argues that if urban sensing participants are co-researchers, sensing systems should enable them to make decisions and take actions to negotiate capture and disclosure. Data control actions are integral to, and embedded within, the sensing process. Participants can take actions on their data whenever they are already interacting with the system, for example, when turning on the system in the morning or when reviewing their data at the end of the day. By providing actions to support flexible privacy processes, urban sensing systems can move away from the pitfall of relying entirely on configuration [51] and move towards data control decisions as a natural component of participant actions.

Research groups may provide guidelines for discretion and sharing, but for campaigns with particularly sensitive data, systems may need to support individual in-situ privacy decisions. Individual regulation of disclosure preferences can address both the highly personal nature of privacy preferences and broader issue of power imbalances and other imperfections in group decision-making [7]. After research groups have discussed default settings for discretion and sharing throughout the data life cycle, participants can define their comfort with data collection and sharing according to situation [20], location [45], and culture [44, 52]. Individuals can also adjust for changing sensitivities and needs over time. Examples of design projects to encourage participant autonomy include:

***Discretion tools*:** Giving participants a selection of "discretion tools" can enable individuals to make fine-grained decisions about their data. An example might be integrating face detection and blurring tools into a system's data analysis interface. Supporting face detection and blurring makes it easy for participants to anonymize images of third parties collected

during a photography campaign. Development of algorithms to give participants the ability to create small amounts of new geo-temporal data that match the participant's 'average' or 'expected' location trace could provide another discretion tool. Participants could substitute 'new' data for periods in which they did not wish to disclose their location. Creating such tools is an outstanding design challenge.

***Selective retention*:** In order to protect individuals' willingness to share data, user interfaces must support manual deletion of data at any granularity. This allows participants to banish sensitive data from the system entirely. Participants could also use system interfaces to indicate internal retention dates for their personal data collection, enabling automatic deletion of internal data after a specified period. Design challenges include building mechanisms to enforce both manual and automatic retention limits.

***Negotiating with outside parties*:** Once participants share data with external applications, retention and reuse policies become harder to enforce. Urban sensing systems can facilitate monitoring of data shared with outside parties or programs through mechanisms for participants to audit outside use of sensing data. Techniques such as performing a hash to compare participant data sets with third party data sets provide a technical approach to test for compliance with participant representations and retention requirements. But participants must also rely on social contracts (or even legal recourse) to negotiate with parties with whom they have shared data.

E. Synergy between policy and technology

Software (or hardware, for that matter) cannot be the sole answer to ethical data collection and use [5]. Effective participatory privacy regulation must combine technological approaches with institutional policies to enable and enforce protective actions. Policy refers to guidelines or regulations to encourage user engagement or safeguard participant data. While some policy is mandated by law or university regulations [30], groups can also agree to guidelines at the institutional or project level. Policy is an important part of the research process: it can help research groups work through conflict and make decisions [31]. Urban sensing technologies must support both research processes and any resulting policy.

Responsibility for policy setting, as part of research decision-making, is shared between researchers and users [32]. A participatory policy approach should encourage project leaders and participants to work alongside designers to write and enforce project guidelines. In addition, discussions with project participants should influence internal compliance policies. Policy will compliment technology design and individual participant decisions to create an urban sensing environment where privacy regulation is an important component of system interaction.

Combining policy and technology challenges designers and participants to determine which issues are best addressed by policy or technology. Authoring policy to support technology and designing technology to support policy are also difficult challenges. For example, how do we design storage and back-up that fully supports strict data retention policies? Finally, campaigns may require different areas of expertise to create appropriate policies and technologies. In just one example, public health campaigns could require consultation of experts in protecting medical records. Combining policy and technology entails all of the challenges of interdisciplinary cooperation.

V. CONCLUSION

Privacy regulation processes within urban sensing systems include participant negotiation of data capture, presentation, and disclosure. Because the needs and preferences of an individual change according to social situation, these negotiations cannot be separated from a person's context. This is why we argue that privacy must be a participatory process to account for both individual preferences and social settings.

Evaluating the effectiveness of this approach, and the resulting software and policy, is challenging future work. How deeply, and under what conditions, do participants engage with participatory sensing systems? How do urban sensing participants negotiate decisions to capture, share, and retain their data, and how well does participatory privacy regulation support this privacy and sharing decision-making? In addition to qualitative survey, we plan to evaluate participation in our urban sensing campaigns to compare individuals' privacy actions to their degree of involvement, measured according to amount of data gathered, and length and frequency of involvement in data gathering.

Though we know tensions between data sharing and protection to be critical in urban sensing projects, we ultimately believe that such research must emphasize participation over restriction as a response to privacy ethics. Restrictions based on preset privacy configurations or designer attempts to eliminate all potential disclosure harms will limit the quality of the data communities collect and the results they achieve. Reframing privacy regulation processes as integral to project participation integrates privacy into the whole of project design – and project success. We argue that by finding a balance between privacy and participation, participants can responsibly use embedded networked sensing systems for their research, empowerment and documentary potential.

REFERENCES

[1]R. A. Hankins, E. Etelapera, Y. Ma, T. Mielikainen, and D. Racz, "Everybit: A Community Platform for Experimenting with Mobile Data," in *IEEE Workshop on Mobile Computing Systems and Applications*, 2008.

[2]S. B. Eisenman, N. D. Lane, E. Miluzzo, R. A. Peterson, G. S. Ahn, and A. T. Campbell, "MetroSense Project: People-Centric Sensing at Scale," in *ACM SenSys Workshop on World-Sensor-Web (WSW'2006)*, 2006.

[3]J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, "Participatory sensing," in *World Sensor Web Workshop, ACM Sensys 2006* Boulder, CO, 2006.

[4]N. Eagle and A. Pentland, "Reality mining: sensing complex social systems," *Personal and Ubiquitous Computing,* pp. 255-268, 2006.

[5]E. Paulos, R. Honicky, and E. Goodman, "Sensing Atmosphere", Workshop on Sensing on Everyday Mobile Phones," in *ACM Conference on Embedded Networked Sensor Systems (SenSys 2007)*, 2007.

[6]E. Agapie, G. Chen, D. Houston, E. Howard, J. Kim, M. Y. Mun, A. Mondschein, S. Reddy, R. Rosario, J. Ryder, A. Steiner, J. Burke, D. Estrin, and M. H. M. Rahimi, "Seeing Our Signals: Combining location traces and web-based models for personal discovery," in *9th IEEE Workshop on Mobile*

Computing Systems and Applications (HotMobile 2008) Napa Valley, CA, 2008.
[7] M. Cargo and S. L. Mercer, "The value and challenges of participatory research: strengthening its practice," *Annual Review of Public Health,* vol. 29, 2008.
[8] E. Byrne and P. M. Alexander, "Questions of ethics: Participatory information systems research in community settings," in *SAICSIT* Cape Winelands, South Africa, 2006, pp. 117-126.
[9] S. Pilemalm and T. Timpka, "Third generation participatory design in health informatics - making user participation applicable to large-scale information system projects," *Journal of Biomedial Informatics,* 2007 (in press).
[10] J. Corburn, "Bringing local knowledge into environmental decision making: Improving urban planning for communities at risk," *Journal of Planning Education and Research,* vol. 22, pp. 120-133, 2003.
[11] A. D. Joseph, "Works in progress: security and privacy in pervasive computing," *Pervasive Computing,* vol. 6, pp. 73-75, 2007.
[12] D. Anthony, D. Kotz, and T. Henderson, "Privacy in location-aware computing environments," *Pervasive Computing,* vol. 6, pp. 64-72, 2007.
[13] G. R. Hayes, E. S. Poole, G. Iachello, S. N. Patel, A. Grimes, G. D. Abowd, and K. N. Truong, "Physical, social and experiential knowledge in pervasive computing environments," *Pervasive Computing,* vol. 6, pp. 56-63, 2007.
[14] J. Hong and M. Satyanarayanan, "Security & privacy," *Pervasive Computing,* vol. 6, pp. 15-17, 2007.
[15] A. Surie, A. Perrig, M. Satyanarayanan, and D. J. Farber, "Rapid trust establishment for pervasive personal computing," *Pervasive Computing,* vol. 6, pp. 24-30, 2007.
[16] M. S. Ackerman and L. Cranor, "Privacy critics: UI components to safeguard users' privacy," in *Conference on Human Factors in Computing Systems CHI'99*: ACM Publications, 1999, pp. 258-259.
[17] D. H. Nguyen and E. D. Mynatt, "Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems," Georgia Institute of Technology GIT-GVU-02-16, 2002.
[18] C. Jensen, J. Tullio, C. Potts, and E. D. Mynatt, "STRAP: A Structured Analysis Framework for Privacy," Georgia Institute of Technology, Atlanta, GA 2005.
[19] S. Patil and J. Lai, "Who gets to know what when: configuring privacy permissions in an awareness application," in *SIGCHI Conf. Human Factors in Computing Systems (CHI 05)* Portland, Oregon: ACM Press, 2005, pp. 101–110.
[20] J. Waldo, H. S. Lin, and L. I. Millett, *Engaging privacy and information technology in a digital age*. Washington, D.C.: The National Academies Press, 2007.
[21] H. Burkert, "Privacy-enhancing technologies: Typology, critique, vision," in *Technology and privacy: The new landscape*, P. E. Agre and M. Rotenberg, Eds. Cambridge, MA and London: The MIT Press, 1998, pp. 125-142.
[22] L. Bannon, "Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing," *CoDesign,* vol. 2, pp. 3-15, 2006.
[23] J.-F. Blanchette and D. G. Johnson, "Data retention and the panoptic society: the social benefits of forgetfulness," *The Information Society,* vol. 18, 2002.
[24] A. Acquisti, "Privacy in electronic commerce and the economics of immediate gratification," in *ACM Conference on Electronic Commerce*: ACM, 2004, pp. 21-29.
[25] M. Brown and R. Muchira, "Investigating the relationship between Internet privacy concerns and online purchase behavior," *Journal of Electronic Commerce Research,* vol. 5, pp. 62-70, 2004.
[26] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *2000 ACM SIGMOD International Conference on Management of Data*, 2000, pp. 439-450.
[27] S. E. Fienberg, "Privacy and confidentiality in an e-commerce world: Data mining, data warehousing, matching and disclosure limitation," *Statistical Science,* vol. 21, pp. 143-154, 2006.
[28] L. Palen and P. Dourish, "Unpacking "privacy" for a networked world," in *CHI 2003*. vol. 5 Ft. Lauderdale, FL: ACM, 2003, pp. 129-136.
[29] G. Iachello and J. Hong, "End-user privacy in human-computer interaction," *Foundations and Trends in Human-Computer Interaction,* vol. 1, pp. 1-137, 2007.
[30] R. Anderson and T. Moore, "The Economics of Information Security," *Science,* vol. 314, pp. 610-613, 27 October 2006.
[31] A. Acquisti and R. Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," in *Privacy Enhancing Technologies 2006*, 2006.
[32] K. B. Frikken and M. J. Atallah, "Privacy preserving route planning," in *ACM Workshop on Privacy in the electronic society*: ACM, 2004, pp. 8-15.
[33] J. A. Halderman, B. Waters, and E. W. Felten, "Privacy management for portable recording devices," in *ACM Workshop on Privacy in the electronic society*: ACM, 2004, pp. 16-24.
[34] C. Tronoso, G. Danezis, E. Kosta, and K. Preneel, "Pripayd: privacy friendly pay-as-you-drive insurance," in *ACM Workshop on Privacy in the electronic society*: ACM, 2007, pp. 99-107.
[35] L. P. Cox, A. Dalton, and V. Marupadi, "SmokeScreen: flexible privacy controls for presence-sharing," in *International conference on Mobile systems, applications and services*, 2007, pp. 233-245.
[36] J. E. Cohen, "Privacy, Visibility, Transparency, and Exposure," *University of Chicago Law Review,* vol. 75, 2008.
[37] H. Nissenbaum, "Privacy as contextual integrity," *Washington Law Review,* vol. 79, pp. 119–158, 2004.
[38] P. G. Lange, "Publicly private and privately public: Social networking on YouTube," *Journal of Computer-Mediated Communication,* vol. 13, p. n.d., 2007.
[39] B. Friedman, P. H. Kahn Jr., J. Hagman, and R. L. Severson, "The watcher and the watched: Social judgments about privacy in a public place," *Human-Computer Interaction,* vol. 21, pp. 235-272, 2006.
[40] M. Madden, S. Fox, A. Smith, and J. Vitak, "Digital footprints: online identity management and search in the age of transparency," Pew Internet & American Life Project, Washington, DC 2007.
[41] A. Lenhart and M. Madden, "Teens, Privacy and SNS," Pew Internet & American Life Project, Washington, DC April 18 2007.
[42] M. R. Curry, D. J. Phillips, and P. M. Regan, "Emergency response systems and the creeping legibility of people and places," *The Information Society,* vol. 20, pp. 357-369, 2004.
[43] V. Bellotti, "Design for privacy in multimedia computing and communications environments," in *Technology and privacy: The new landscape*, P. E. Agre and M. Rotenberg, Eds. Cambridge, MA and London: The MIT Press, 1998, pp. 63-98.
[44] I. Altman, "Privacy regulation: culturally universal or culturally specific?," *Journal of Social Issues,* vol. 33, pp. 66-84, 1977.
[45] H. Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law and Philosophy,* vol. 17, pp. 559-596, November 1998.
[46] M. A. Shields, "Criminal prosecution of video or photographic voyeurism," in *American Law Reports 5th*. vol. 120: West Group, 2004, p. 337.
[47] A. M. Swarthout, "Eavesdropping as violating right of privacy," in *American Law Reports 3rd*. vol. 11: West Group, 1967, p. 1296.
[48] D. Schuler and A. Namioka, *Participatory Design: Principles and Practices*. Hillsdale, NJ: Lawrence Erlbaum Associates, 1993.
[49] J. Gregory, "Scandinavian Approaches to Participatory Design," *International Journal of Engineering Education,* vol. 19, 2003.
[50] A. Joki, "Campaignr."
[51] S. Lederer, J. I. Hong, and A. K. Dey, "Personal privacy through understanding and action: five pitfalls for designers," *Pers Ubiquit Comput,* vol. 8, pp. 440–454, 2004.
[52] R. Capurro, "Privacy. An Intercultural Perspective," *Ethics and Information Technology,* vol. 7, pp. 37-47., 2005.