University of Massachusetts - Amherst
ScholarWorks@UMass Amherst

Ethics in Science and Engineering National Clearinghouse

Science, Technology and Society Initiative

6-25-2008

Achieving Participatory Privacy Regulation: Guidelines for CENS Urban Sensing

Katie Shilton
University of California - Los Angeles

Jeffrey A. Burke
University of California - Los Angeles

Deborah Estrin
University of California - Los Angeles

Mark Hansen
University of California - Los Angeles

Mani B. Srivastava
University of California - Los Angeles

Follow this and additional works at: http://scholarworks.umass.edu/esence

Part of the Library and Information Science Commons, and the Science and Technology Studies Commons

Recommended Citation
Shilton, K., Burke, J., Estrin, D., Hansen, M., and Srivastava, M. "Achieving Participatory Privacy Regulation: Guidelines for CENS Urban Sensing" (June 25, 2008). *Center for Embedded Network Sensing. Technical Reports*. Paper 62. http://repositories.cdlib.org/cens/techrep/62

This Other is brought to you for free and open access by the Science, Technology and Society Initiative at ScholarWorks@UMass Amherst. It has been accepted for inclusion in Ethics in Science and Engineering National Clearinghouse by an authorized administrator of ScholarWorks@UMass Amherst. For more information, please contact scholarworks@library.umass.edu.

Achieving Participatory Privacy Regulation: Guidelines for CENS Urban Sensing

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

June 25, 2008

Center for Embedded Networked Sensing
University of California Los Angeles
{kshilton, destrin, mbs}@ucla.edu, jburke@remap.ucla.edu, cocteau@stat.ucla.edu

Organization of This Report 2
Getting Started 3
Introduction: Participatory Privacy Regulation 5
Why Worry? 7
Existing Toolkit 7
Guideline I: Participant Primacy 9
Problem and Goal Specification 11
Data Collection and Analysis 12
Privacy Protection 12
Beyond the Matrix 12
Feature Examples 13
Guideline II: Participatory Design 14
Achieving Participatory Design 15
The Trouble with "Community" 16
Participatory Design for Privacy 18
Privacy Design Flow Chart 19
Mitigating Pressure Points and Setting Privacy Defaults 21
Avoiding Privacy Pitfalls 21
Feature Examples 22
Design Case Studies 23
Guideline III: Participant Autonomy 25
Mapping a Campaign 25
Control Over Capture 27
Control Over Storage 28
Control Over Processing 28
Control Over Sharing 28
Control Over Republishing 29
Control Over Retention and Reuse 29
Feature Examples 30
Guideline IV: Minimal and Auditable Information 32
Minimal Information and Targeted Capture 32
Audit and Compliance 32
Feature Examples 33
Guideline V: Synergy between Policy and Technology 34
Campaign Documentation, Internal Review Board (IRB) and Informed Consent 36
Documenting Campaigns 36
Complying with IRB requirements 36
Informed Consent 36
Conclusion 38
Possibility, Not Restriction 38
References 39

Urban and participatory sensing projects involve many different goals, technologies, and users. Managing privacy and data protection requirements for projects as different as academic dietary studies using image capture and grassroots community assets projects tracking location traces requires different system and policy adaptations.

Determining the privacy concerns of any given urban sensing project is a complicated task. Designing for privacy requires weighing appropriate measures for a wide variety of individual and group needs, including location privacy, sharing of photographs and images, and questions of identity, anonymity, and pseudonymity. CENS urban sensing projects range between personal sensing, top-down sensing, and grassroots sensing projects, and each project works with different forms of data, different populations, and therefore different sets of privacy concerns. Sometimes restriction is necessary; in other cases, transparency and accountability are the best responses. This technical report is designed to help CENS designers make those choices.

How can CENS designers grapple with the privacy concerns raised by each new urban sensing project? Designers need a set of tools to map applicable privacy concerns, to grapple with both existing techniques for and innovative responses to protecting privacy, and to work with participant communities to alleviate some of these concerns.

Organization of This Report

This technical report is intended to help CENS urban sensing researchers incorporate participation and respect privacy while conducting research about people. The goal is to provide a framework by which to assess an appropriate level of participation and meaningful policy and technical responses to privacy concerns. By keeping in mind the five guidelines outlined here, system developers can respond to participant needs and balance the benefits of data gathering with individual and group privacy.

The Introduction defines and describes *participatory privacy regulation*: the approach to privacy design taken at CENS. Sections I-V provide descriptions and planning tools for each of the five parts of participatory privacy regulation:

I. Participant Primacy
II. Participatory Design
III. Participant Autonomy
IV. Minimal and Auditable Data
V. Synergy Between Policy and Technology

The first three guidelines summarize principles for working with campaign participants and technology consumers. The last two guidelines summarize principles for working with systems and data. Section VI provides information important to any research project involving human subjects, including details on documenting campaigns, gaining informed consent, and working with UCLA's Internal Review Board (IRB).

Getting Started

Urban Sensing researchers should briefly review these checklists of guidelines during the campaign and architecture design process.

Campaigns

- ❑ Discuss where a campaign will fall on the spectrum of participation. (*See page 5*)
- ❑ Decide upon the nature of participant, domain researcher, and system researcher roles in the campaign. (*See page 10*)
- ❑ Consult participatory design guidelines appropriate to the campaign's level of participation. (*See page 15*)
- ❑ Plan a campaign's privacy requirements. (*See page 25*)
- ❑ Encourage participant discretion when dealing with third party data. (*See page 26*)
- ❑ Decide where policy (guidelines for researchers and participants) is needed to address participation and privacy issues not addressed by architecture. (*See page 34*)
- ❑ Document campaign decisions, complete IRB requirements and create readable informed consent documents. (*See page 36*)

Architecture

- ❑ Consider the participatory nature of a campaign and the sensitivity of data to be collected and decide to make systems more or less restrictive. (*See page 21*)
- ❑ Make the data life cycle – and decisions about that life cycle – legible to participants. (*See page 25*)
- ❑ Sensors should be able to be turned off and on or otherwise controlled by participants. (*See page 25*)
- ❑ Discuss whether and how sensors could be made obvious to allow third parties to avoid unwanted capture. (*See page 27*)
- ❑ Allow for confidential usernames and confidential use by participants. (*See page 28*)
- ❑ Restrict third party access to a participant's data. (*See page 28*)
- ❑ Allow easy masking, altering, or deleting of data. (*See page 28*)
- ❑ System should require explicit participant action, such as authorizing feed sharing, to share or republish data. (*See page 28*)
- ❑ Allow participant to decide how long their data is retained. (*See page 29*)
- ❑ Allow participant to decide which, if any, data can be reused or repurposed. (*See page 29*)
- ❑ Enable participant to check retention and reuse of data shared with outside parties. (*See page 29*)

Participatory Sensing Research Group

- ❑ Introduce new researchers to participation and privacy guidelines.

- ❑ Regularly check for compliance with internal reuse guidelines. (*See page 32)*
- ❑ Regularly check for compliance with internal retention guidelines. (*See page 32)*

Introduction: Participatory Privacy Regulation

Participatory privacy regulation stems from dual requirements: giving participants in CENS urban sensing systems control over data gathering and sharing according to their context and preferences; and giving participants a meaningful role in the processes of research planning, data collection, and data analysis. 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, CENS system designers should consider participatory privacy regulation from the very beginning of the design process.

What do we mean by participatory privacy regulation? **Participation** is a process of engagement in research or system design. Participation can range from passive to fully self-mobilized, and degree of participation is dependent upon the roles and activities in which a participant is involved.[1]

- ***Top-down sensing*** projects leave academic researchers and designers in charge of most research and system design.
- ***Grassroots sensing*** projects involve community participants in data collection and analysis, and ask participants to make decisions about sharing, retaining, and repurposing their data.
- ***Participatory sensing research*** projects involve research participants in design of the research methods and goals in addition to sensing and data analysis.

Privacy is a process of selective control of access to the self,[2] or to information about the self.[3] Privacy acquires specific – and variable – meaning in specific circumstances and settings.[4] It includes elements of negotiating boundaries, identity, and time.[5] Privacy includes both descriptive and normative concepts: private information can either be inaccessible to others, or should be inaccessible to others.[6] Privacy regulation can be a process of enforcing personal

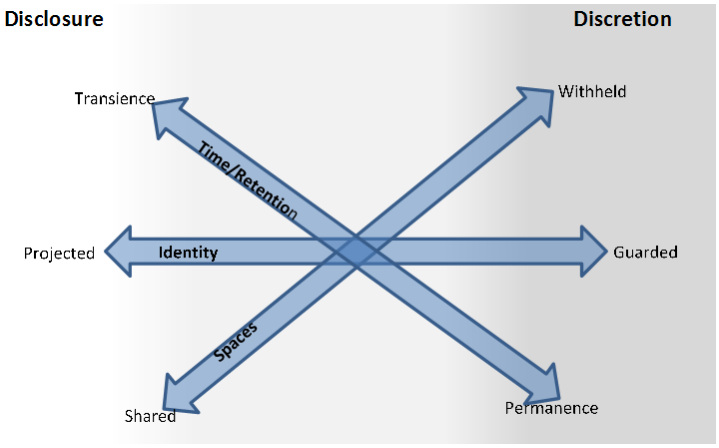

Figure 1: Factors in privacy decision-making

[1] E. Byrne and P. M. Alexander, "Questions of Ethics: Participatory Information Systems Research in Community Settings," SAICSIT (Cape Winelands, South Africa: 2006), vol.
[2] Irwin Altman, "Privacy Regulation: Culturally Universal or Culturally Specific?," Journal of Social Issues 33.3 (1977), Leysia Palen and Paul Dourish, "Unpacking "Privacy" For a Networked World," CHI 2003 (Ft. Lauderdale, FL: ACM, 2003), vol. 5.
[3] James Waldo, Herbert S. Lin and Lynette I. Millett, Engaging Privacy and Information Technology in a Digital Age (Washington, D.C.: The National Academies Press, 2007).
[4] Altman, "Privacy Regulation: Culturally Universal or Culturally Specific?.", Batya Friedman, Peter H. Kahn Jr., Jennifer Hagman and Rachel L. Severson, "The Watcher and the Watched: Social Judgments About Privacy in a Public Place," Human-Computer Interaction 21 (2006), H. Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public," Law and Philosophy 17.5-6 (1998).
[5] Palen and Dourish, "Unpacking "Privacy" For a Networked World."
[6] Waldo, Lin and Millett, Engaging Privacy and Information Technology in a Digital Age.

boundaries (including measures taken for safety, or to protect seclusion) or a method of portraying particular identities (such as boss, spouse, or student).[7] The customs of a society, place, or space have ongoing influence on these personal decisions. An individual's 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.[8] 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.[9] Figure 1 illustrates the continuums that individuals may take into account during privacy decision-making and regulation.

Decisions about disclosure and discretion are integral to the sensing research process, as well. Making decisions about what data sensors will capture is part of defining data collection requirements. Choices 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. The relationship of privacy to the overall process of participation in urban sensing is illustrated in Figure 2.

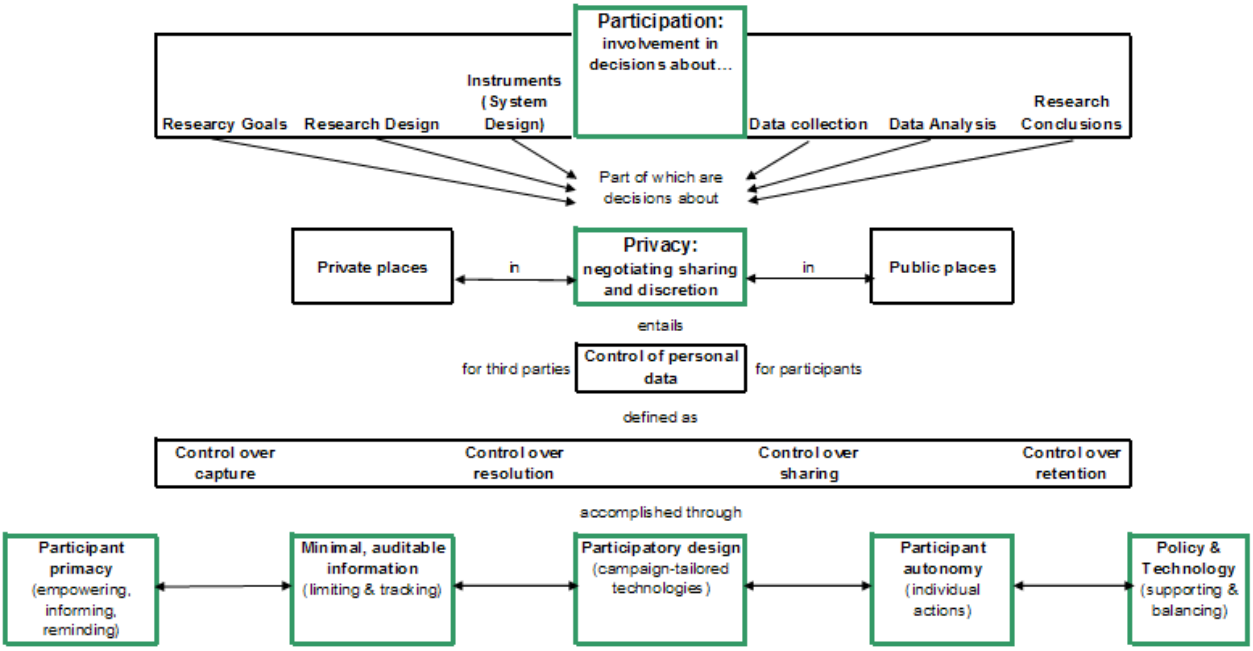

Figure 2: Relationship of participation and privacy

[7] Palen and Dourish, "Unpacking "Privacy" For a Networked World."
[8] Helen Nissenbaum, "Privacy as Contextual Integrity," Washington Law Review 79.1 (2004).
[9] Patricia G. Lange, "Publicly Private and Privately Public: Social Networking on Youtube," Journal of Computer-Mediated Communication 13.1 (2007).

Why Worry?

Participation in the entire sensing process – from setting campaign goals to analyzing sensor data – 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. By considering privacy decision-making throughout participatory sensing projects, the five principles of participatory privacy regulation incorporate disclosure decisions as part of participants' commitment to a project.

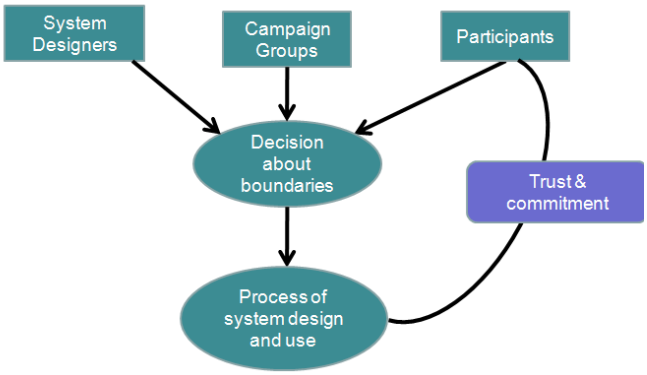

Figure 3: Participation as a component of commitment

Existing Toolkit

Participatory privacy regulation is designed to help CENS designers choose from and expand an existing toolkit for system privacy. A wide variety of existing technical approaches to privacy design include:

- privacy warning, notification, or feedback systems;[10]
- methods for identifying privacy vulnerability in information systems;[11]
- systems that enable user choices about data sharing;[12]
- identity management systems;[13]
- and selective retention systems.[14]

Technical approaches to protecting user data include encryption, privacy-enhancing technologies (PETs), and statistical anonymization of data.[15] Additional previous work explores data retention or its opposite, systematic "forgetting."[16]

---

[10] Gillian R. Hayes, Erika Shehan Poole, Giovanni Iachello, Shwetak N. Patel, Andrea Grimes, Gregory D. Abowd and Khai N. Truong, "Physical, Social and Experiential Knowledge in Pervasive Computing Environments," Pervasive Computing 6.4 (2007); Mark S. Ackerman and Lorrie Cranor, "Privacy Critics: UI Components to Safeguard Users' Privacy," Conference on Human Factors in Computing Systems CHI'99 (ACM Publications, 1999); David H. Nguyen and Elizabeth D. Mynatt, Privacy Mirrors: Understanding and Shaping Socio-Technical Ubiquitous Computing Systems (Georgia Institute of Technology, 2002).

[11] Carlos Jensen, Joseph Tullio, Colin Potts and Elizabeth D. Mynatt, STRAP: A Structured Analysis Framework for Privacy (Atlanta, GA: Georgia Institute of Technology, 2005).

[12] Denise Anthony, David Kotz and Tristan Henderson, "Privacy in Location-Aware Computing Environments," Pervasive Computing 6.4 (2007).

[13] Sameer Patil and Jennifer Lai, "Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application," SIGCHI Conf. Human Factors in Computing Systems (CHI 05) (Portland, Oregon: ACM Press, 2005).

[14] Hayes, et al, "Physical, Social and Experiential Knowledge in Pervasive Computing Environments."

Despite these existing approaches, building *systems* that protect user privacy remains a challenge. In a survey of technical approaches to privacy in human-computer interaction, Iachello and Hong 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.[17] The five principles of participatory privacy regulation are design to help CENS researchers navigate variable, system-wide privacy requirements on a campaign-by-campaign basis.

[15] Waldo et al, Engaging Privacy and Information Technology in a Digital Age; Herbert Burkert, "Privacy-Enhancing Technologies: Typology, Critique, Vision," Technology and Privacy: The New Landscape, eds. Philip E. Agre and Marc Rotenberg (Cambridge, MA and London: The MIT Press, 1998).
[16] J.-F. Blanchette and D.G. Johnson, "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness," The Information Society 18.33-45 (2002); Liam Bannon, "Forgetting as a Feature, Not a Bug: The Duality of Memory and Implications for Ubiquitous Computing," CoDesign 2.1 (2006).
[17] Giovanni Iachello and Jason Hong, "End-User Privacy in Human-Computer Interaction," Foundations and Trends in Human-Computer Interaction 1.1 (2007).

Guideline I: Participant Primacy

Participant primacy means CENS designers, and CENS urban sensing systems, should help users take on the role and responsibilities of researchers. If users are going to be part of the process of making decisions about disclosure and discretion, they should not only be well-informed enough about the system operations and data collection to make these decisions, they should feel responsible for making these decisions because they are an integral part of the research process.

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.

The first challenge for CENS designers is incorporating the participation of users in a variety of roles. Users can participate in any combination of campaign planning, sensing system design, data collection, data analysis, and drawing research conclusions. A matrix of participation based upon the roles and activities of participants, system researchers, and domain researchers is illustrated in Table 1.

Participatory Sensing Matrix	Top-Down Sensing		Participatory Sensing		Grassroots Sensing
	1	2	3	4	5
Problem and goal specification:					
Who instigates research?	DR	DR	DR & P	DR & P	P
Who decides goals?	DR	DR	DR & P	P	P
Who designs methods?	DR	DR	DR & P	P	P
Who designs systems?	SR	SR	SR	SR & P	P
Who controls output?	DR & SR	DR & SR	All	P	P
Data collection and analysis:					
Who defines data?	DR & SR	DR & SR	DR & SR	All	P
Who collects data?	P	P	P	P	P
Who analyzes data?	DR & SR	DR & SR	DR & SR	All	P
Privacy protection:					
Who defines privacy?	DR & SR	DR & SR	All	All	P
Who plans system specs for privacy?	SR	SR	SR	SR & P	P
Who takes privacy actions?	DR & SR	All	All	All	P

Table 1: Possibilities for Participant Roles

DR = Domain Researchers
SR = System Researchers
P= Participants

The overlap of roles in the participation matrix above points to the fuzziness of the lines between participant, systems researchers, and domain researchers. During CENS pilots and perhaps some CENS projects, systems researchers will also take on the roles of domain researchers and participants. Professional social science researchers may become systems researchers as well when they partner with CENS and participate in decisions about how to address design requirements. And in participatory sensing projects which fully involve outside community members, the participants may become both domain researchers and systems researchers. The blurring of roles suggests that a passive-to-self-mobilized continuum is not a linear progression, but a loop. In a fully self-mobilized project, participants become the domain and systems researchers, and the research scenario becomes analogous to CENS designers building systems used for internal pilots.

Problem and Goal Specification

Part of participation in sensing projects is participation in the decision-making behind the projects. Are participants meaningfully involved in all aspects of problem and goal specification? In top-down sensing projects, participants make few or none of these decisions. In grassroots sensing, participants initiate and design the research and make decisions by consensus.[18]

- **Instigating research**: Do participants also serve as leaders in organizing a research effort? Do they participate in activities related to starting and organizing a research project? To what degree do participants rely on a few leaders to instigate the research, or distribute the organization functions broadly among community members?
- **Deciding research goals**: Does the participant community organize to decide upon the goals of the research? Or are research goals set by parties external to the participant community? To what extent are decisions about research goals made with community consensus?
- **Designing research:** Does the participant community have control over decisions about what data will be collected, when, and why? Does the participant community have control over decisions about how the data will be analyzed, published, and understood? Does it have control over where data will be stored, and how data will be shared?
- **Controlling research output**: Does the community have control over what the research outputs will be, and who will control, publish, or own the research outputs? To what extent are research outputs decided with community consensus?

There are natural tensions between CENS technology development and completely community-controlled and instigated research. Because CENS is taking the initiative to develop particular sensing technologies, there is a push to find research projects to fit those technologies. Similarly, the limits of CENS technologies, such as the limits of kinds of data they can collect, shape research goals, design, and output.

[18] Byrne and Alexander, "Questions of Ethics: Participatory Information Systems Research in Community Settings."

Data Collection and Analysis

Participation also depends on involvement in the sensing process. How widely and justly distributed is participation in the data gathering throughout the participant community? Participation in data collection and analysis might include:

- **Participation in defining data:** How is "data" defined? Is local knowledge - knowledge held by community members and developed through experience living within that time, place, and community[19] – meaningfully represented in the notion of data? Is subjective experience included in a campaign's definition of data?
- **Participation in data collection:** Are participants meaningfully involved in data collection? Do participants make decisions about when, where, and how data is collected?
- **Participation in data analysis:** Are participants meaningfully involved in data analysis? Who decides how data is represented? Who decides what is considered 'good' data? Who decides upon reputation framework? Is discretion with third party data considered a part of reputation?

Privacy Protection

Finally, decisions about privacy factor into participation in sensing projects. Questions of who defines privacy and related data pressure points, who plans resulting system specifications, and who takes privacy-protecting actions during the sensing project all reflect on the participatory nature of a project.

- **Defining privacy:** Because privacy is an identity-regulation process that varies greatly according to situation,[20] location,[21] and culture,[22] privacy needs and concerns must be defined by participants. Because participants are likely to have different privacy thresholds, research projects must be flexible to allow for varying privacy protections.
- **Planning system specifications for privacy:** Participant-defined privacy needs can be operationalized by envisioning the entire research process and identifying privacy "pressure" points. See section … for further details.
- **Taking privacy-protecting actions:** A campaign should allow for a variety of privacy-protecting actions, ranging from selective participation in data capture to selective retention, sharing, or publication of data. Participants should also be able to alter the resolution of their data to preserve their confidentiality or privacy.

Beyond the Matrix

Questions that CENS designers might ask, but which do not fit neatly into a matrix,[23] include:

---

[19] Jason Corburn, "Bringing Local Knowledge into Environmental Decision Making: Improving Urban Planning for Communities at Risk," Journal of Planning Education and Research 22 (2003).
[20] Waldo, et al, Engaging Privacy and Information Technology in a Digital Age.
[21] Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public."
[22] Altman, "Privacy Regulation: Culturally Universal or Culturally Specific?"; Rafael Capurro, "Privacy. An Intercultural Perspective," Ethics and Information Technology 7 (2005).
[23] Giacomo Rambaldi, Robert Chambers, Mike McCall and Jefferson Fox, "Practical Ethics for PGIS Practitioners, Facilitators, Technology Intermediaries and Researchers," Participatory Learning and Action 54.April (2006): 108.

- What will change in a community as a result of a sensing project?
- Who benefits from the changes?
- What is the cost of those changes? Who will bear the cost?
- Who gains and who loses from a sensing project?
- Who is empowered and who is disempowered?

Feature Examples

A number of different system features could contribute to participant primacy in an urban sensing project. Any feature that encourages user responsibility, decision-making, and action can be said to encourage participant primacy. Some examples might include:

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.

Reputation systems: Project leaders and designers can use system software to promote responsible data practices. For example, evaluations of participants' contributions 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: 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 or eavesdropping.

Flexible user authentication: 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. Development of authentication processes that support strong identity as well as anonymous, pseudonymous, and confidential identities may be important for urban sensing.

Guideline II: Participatory Design

Participatory design is a practice that incorporates users as co-designers of a system.[24] As a principle to guide urban sensing, participatory design encourages CENS researchers to incorporate user ideas, feedback and needs to customize and adapt systems on a campaign-by-campaign basis. The urban sensing design process should therefore encourage cooperative design 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).

Why is participatory design important? CENS designs urban sensing systems to use 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.

For example, 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.[25] 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 ongoing group discussion of data needs and disclosure risks. Communities can use immersion in the design process to identify concerns that individuals may miss.

Using a participatory design process, participants and designers can 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.

---

[24] M. J. Muller, "Participatory Design: The Third Space in HCI," Handbook of HCI (Mahway, NJ: Erlbaum, 2003); S. M. Dredger, A. Kothari, J. Morrison, M. Sawada, E. Crighton and I. D. Graham, "Using Participatory Design to Develop (Public) Health Decision Support Systems through GIS," International Journal of Health Geographics 6.53 (2007); Doug Schuler and A. Namioka, Participatory Design: Principles and Practices (Hillsdale, NJ: Lawrence Erlbaum Associates, 1993).

[25] Alessandro Acquisti and Ralph Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," Privacy Enhancing Technologies 2006 (2006); Waldo, et al, Engaging Privacy and Information Technology in a Digital Age.

Achieving Participatory Design

There is a large literature on the processes and challenges of participatory design. There are a number of specific design techniques that CENS can use to cooperate with urban sensing participants, including observation, interview, focus groups, prototyping …[26] Rather than present detailed methods here, we will outline some of the higher-level guidelines to system development laid out by the participatory design movement.

In an article about participatory design and use of GIS systems, Rambaldi et al highlight a number of practical and ethical suggestions for participants and designers.[27] These include:

Motivations

- Examine which, and whose, purpose you are pursuing
- Recognize that the researcher's presence is not politically neutral
- Foreground local values, needs and concerns
- Avoid causing tensions or conflict in a community

Conduct with participants

- Strive for honesty and openness
- Obtain informed consent from participants
- Avoid raising false expectations
- Be considerate with participants' time
- Build trust (and invest time and resources to do so)
- Avoid exposing participants to danger
- Don't dictate boundaries
- Avoid repeating activities
- Stimulate learning and information generation rather than mere data extraction
- Focus on local knowledge
- Data gathering is a means, not an end
- Ensure genuine custodianship of results by the participant community
- Ensure that outputs are understood by everyone
- Ensure intellectual property rights for participant community
- Acknowledge informants
- Review and revise findings

Design practices

- Don't rush
- Be flexible with technologies and consider using technologies that can be mastered by participants
- Observe the process
- Select technologies adapted to local conditions and capacities

---

[26] Schuler and Namioka, Participatory Design: Principles and Practices;Muller, "Participatory Design: The Third Space in HCI."

[27] Rambaldi, et al, "Practical Ethics for PGIS Practitioners, Facilitators, Technology Intermediaries and Researchers," 108-12.

- Don’t sacrifice local knowledge in the name of precision
- Be ready to deal with new realities which will emerge during the process

Another issue in participatory design is who to work with. Participants will have limited time and interest for participatory design. Compounding the complexity of finding volunteers for participatory design is that no set of volunteers will be neutral representatives of their “community.”

The Trouble with “Community”

Community” involvement will clearly influence the participatory nature of a sensing project, but we should avoid thinking of “community” as a homogenous group with a uniform level of participation. Within each community will be power structures based upon gender, class, ethnicity, religion or other cultural difference, or upon community-specific factors. Individuals within a community will also have different levels of involvement depending upon time, interest, and patience with the design and development process.[28] Researchers working with community groups must be sensitive to all of the variations of participation within a research group and project. For more on working with community differences, see …

In order to determine whether we are working with a helpful, diverse, and representative subset of a community, designers can ask a few critical questions. By thinking critically about who, in any given community, is needed to ensure the success of a technology project, CENS designers can reach out to stakeholders that can not only improve our design process but help introduce our tools to users. ***Worksheet 1: Selecting Participants*** builds on the work of Rambaldi[29] to suggest questions CENS designers might ask.

[28] Byrne and Alexander, "Questions of Ethics: Participatory Information Systems Research in Community Settings.”
[29] Rambaldi, et al, "Practical Ethics for PGI Practitioners, Facilitators, Technology Intermediaries and Researchers."

Planning for Participation: Who are our partners?		**Who is needed to:**				
Non-academic partners	***Who are they?***	**Ensure respect for values during campaign?**	**Ensure translation of results into action?**	**Ensure scientific, social, and cultural validity?**	**Ensure best use of community assets?**	**Ensure project sustainability?**
Participants						
Participants' support network (parents, family, etc.)						
General public interested in the issue						
Practitioners/service providers who work with participants						
Administrative or political actors who deal with participants or issue						

Participatory Design for Privacy

Once CENS designers have gathered a group of willing co-designers, privacy should be one of the issues addressed by the team. Through careful mapping of research objectives and procedures before sensing begins, researchers and participants can identify ***privacy pressure points:*** junctures during the data life cycle when participants' data might be visible to third parties.[30] It is at these pressure points that participants need options for negotiating how data is captured, represented, and stored.

Privacy pressure points which all campaigns should consider include:

- Identifying where personally identifying information is captured and working on encrypting, securing, or scrubbing that information.
- Issues of bin size where there is risk of individual identification by deduction through aggregation of data.[31]
- Tiers of risk and access for data types (geospatial, image, sound) collected.[32]
- Data retention by outside parties, whether people or processing programs.

Table 2 suggests some of the privacy pressure points that may occur throughout the data life cycle. However, individual campaigns may have different sensitivities, and discussion of these sensitivities before a campaign begins is recommended. Campaign organizers should consider confidentiality and privacy protection at every stage of the research process. This includes recruitment of participants, training staff to respect confidentiality and privacy, data collection, and data transfer, processing, sharing, analysis, publication, and storage.[33]

Data Life Cycle	
Capture	*Data granularity*
↓	
	Confidentiality
Storage	
↓	*Private storage*
Processing	*Authorized processing*
↓	
	Selective deletion and retention
	Protection of third parties
Sharing	*Selective sharing*
↓	
Republishing	*Resolution control*
↓	
Retention	*Internal guidelines*
↓	*External integrity*
Reuse	*Internal guidelines*
	External integrity

Table 2: Pressure points in data life cycle

[30] Definitions of privacy almost always include both something that is being kept private, and someone from whom it is being kept private. (See Waldo, et al, Engaging Privacy and Information Technology in a Digital Age.) Therefore, privacy protection does not come into question until data comes into risk of exposure to a third party.
[31] Waldo, et al, Engaging Privacy and Information Technology in a Digital Age.
[32] Panel on Confidentiality Issues Arising from the Integration of Remotely Sensed and Self-Identifying Data, Putting People on the Map: Protecting Confidentiality with Linked Social-Spatial Data (Washington, DC: National Research Council, 2007).
[33] Panel on Institutional Review Boards Surveys and Social Science Research, Protecting Participants and Facilitating Social and Behavioral Sciences Research (Washington, DC: National Research Council, 2003).

Designers should also be sensitive to the fact that they may not be able to identify all of a campaign's privacy pressure points themselves. Designers may need to do background research and invite the opinions and input of their peers and/or the participant community. Techniques of participatory design such as discussions and role play may be useful in discovering privacy pressure points within a campaign. Because privacy is so personally and situationally defined, the more people that have input into the identification of privacy pressure points, the more likely a designer is to be able to address all relevant issues.

There are also tools in the design literature to help identify privacy pressure points. One popular example is STRAP, a framework for identifying the privacy vulnerabilities of a system.[34] STRAP begins by summarizing "goals," which are define as approximations of system properties. "Vulnerabilities" are hypothetical situations that make fulfillment of a goal impossible.

Once a designer has identified system goals, they must ask a series of questions for each goal:

- What data is captured or accessed for this goal?
- Who are the actors involved in the capture and access?
- What knowledge is derived from this information?
- What is done with the information afterward?

The answers to these questions may point to vulnerabilities for each goal. Jensen et al categorize vulnerabilities with the labels:

- Notice/Awareness
- Choice/Consent
- Security/Integrity
- Enforcement/Redress.[35]

These labels can help designers address system vulnerabilities. Designers should look for vulnerabilities that can be eliminated, and vulnerabilities that can be mitigated.

Privacy Design Flow Chart

The chart below lays out a series of questions for designers to ask and a path to resulting privacy decisions. This charts may be used to lead discussions among designers or with participants about design and privacy within campaigns.

[34] Jensen, et al, STRAP: A Structured Analysis Framework for Privacy.
[35] Ibid.

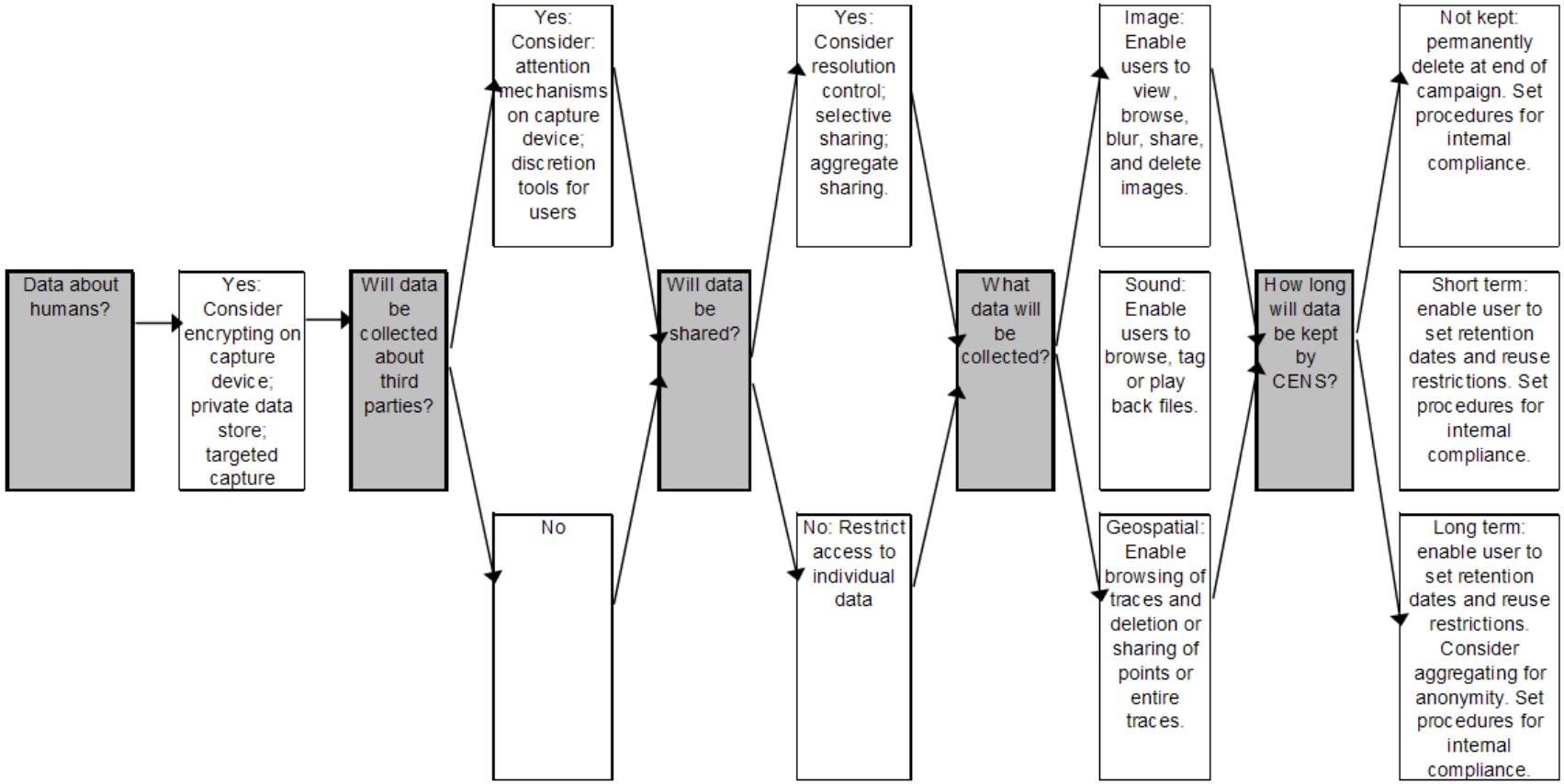

Figure 4: Flow chart for privacy design

Mitigating Pressure Points and Setting Privacy Defaults

Once participants and designers have identified privacy pressure points or vulnerabilities, they can work together through an iterative design process to develop measures for data protection. While participants should be able to make design choices as well as data collection, sharing and retention choices to negotiate their own privacy protections, there is evidence that CENS systems should default to more restrictive privacy settings rather than less. Economic analyses of privacy behaviors and privacy decision-making indicate that system default settings carry an inordinate amount of weight with participants, and that participants have difficulty determining the future costs of relinquishing present privacy.[36]

A number of factors may contribute to participants' willingness to make privacy decisions, ranging from the sensitivity of the data to the personality of the participant. Among these many factors may be the level of participation. Is the tolerable level of involvement with privacy decisions a function of the participatory nature of the project and the investment of the participant in the project? Should we place greater restrictions on data in less-participatory projects?

As Iachello and Hong explain:

> A consensus is slowly building in the research community that privacy-sensitive applications cannot make all data transfers explicit, nor require users to track them all. The related UIs and interaction patterns would simply be too complex and unwieldy. From a data protection viewpoint, experience shows that most data subjects are unable or unwilling to control all disclosures of personal information, and to keep track of all parties that process their personal data.[37]

Avoiding Privacy Pitfalls

Lederer et al suggest a series of privacy "pitfalls" which are classic design mistakes that compromise user privacy.[38] Attention to these pitfalls as CENS designers mitigate privacy pressure points can help us design systems that are both safe and legible to users. Lederer et al's list of pitfalls to avoid, and mechanisms by which to avoid them, are:

Avoid:	***Achieved through:***
Obscuring (Actual and Potential) Information Flow	Helping participants form a mental model of information flow. Using tools such as notifications and logs to alert participants to sharing and data disclosure.
Favoring Configuration Over Action	Designing for privacy choices to be an ongoing part of system participation.

[36] Waldo, et al, Engaging Privacy and Information Technology in a Digital Age; Acquisti and Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook."
[37] Iachello and Hong, "End-User Privacy in Human-Computer Interaction," 98.
[38] Scott Lederer, Jason I. Hong and Anind K. Dey, "Personal Privacy through Understanding and Action: Five Pitfalls for Designers," Pers Ubiquit Comput 8.November (2004).

	Enabling plausible deniability: the reasons a user chooses not to share can be obscured.
Ignoring Course-Grained Control	Allowing participants to turn capture, sharing, retention on and off.
Inhibiting Established Practice	Enabling participants to manage privacy in ways they're already accustomed to, such as turning off their phone, failing to upload data, choosing people with whom to share through buddy lists, etc... Allowing for negotiation of "contextual integrity" – e.g. selectively sharing some kinds of information in certain, user-defined situations.[39]

Feature Examples

A participatory group process will provide design guidelines to tailor software for individual projects. For example, a design process that incorporates users can help CENS designers make decisions about:

Aggregating data: 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. Urban sensing software must be able to adjust capture, storage, and representation of location traces to incorporate such decisions into system default settings.

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 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

[39] Nissenbaum, "Privacy as Contextual Integrity."

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.

Design Case Studies

Top-Down Sensing: DietSense

DietSense is an example of a top-down sensing project.

Participants wear cameras that automatically capture images. Participants are encouraged to wear the cameras all day and participate in continuous image capture. Automated data collection makes accuracy more likely for researchers, but may lead to invasive data collection (i.e. in locker rooms and public restrooms, of third parties who do not wish to be captured, etc.) Participants do not have access to their images until they arrive at the clinic. In the meantime, data is stored on CENS servers.

Once participants arrive at the clinic, they are able to browse their images privately, and have one chance to delete some images, share some images, or delete all images. Once they have decided to share images, those images are given to clinicians, and are beyond further participant control. All participant privacy decisions – either to share or delete – must be made on the spot.

Open design and policy questions for the next iteration of DietSense include:

- Consent: Participants should be given information about the project at a third-grade reading level. Can the CENS team effectively summarize complex privacy decisions and possibilities at a third-grade level?
- Ease of Deletion: At the moment, CENS controls the time and spatial resolution for viewing the photos, and the photographs can only be deleted as single units or in their entirety. Could we give time resolution choices to the participants, without overwhelming them, to easily delete and share photographs from, for example, any given time period?
- Reuse: What should the reuse and long-term retention guidelines be for shared DietSense photographs?

Participatory Sensing: PEIR

PEIR falls somewhere on the spectrum between top-down and grassroots sensing. CENS researchers designed the goals and data collection requirements of the project, but participants may analyze their data, and the benefits of the project are for participants rather than researchers. As PEIR evolves, participants will also be able to take privacy actions such as deleting, aggregating, or manipulating data to be less revealing.

PEIR participants carry GPS-enabled mobile phones that automatically capture location traces while Campaignr is running. Participants are encouraged to capture data continuously. No other data is captured by the phones.

Participants have private access to their location traces from their home computers through a web-based interface. They may use a confidential username and access their encrypted data. Open design and policy questions for the next iteration of PEIR include data sharing and retention defaults, as well as how to enable individual control over data resolution, selective sharing, and selective retention.

Participatory Research: Walkability, Bikeability, and CycleSense

CENS pilot walk- and bike-ability projects approach participatory research by tailoring CENS technologies to help achieve community-specified goals. Los Angeles nonprofit Livable Places incorporated CENS mobile sensing technologies into their recent "Making the Connections" neighborhood walkability campaigns. Participants carried mobile phones while walking or biking through Los Angeles neighborhoods. Participants used the phones to photograph barriers or difficulties for pedestrians and bikers in these neighborhoods. After the campaign, Livable Places was able to document and map these impediments to walking and biking using the geotagged photographs collected by participants. This data will become part of a final plan to connect the target neighborhoods with the city's Gold Line subway route.

Building on this experience, the urban sensing team is currently developing the CycleSense system with the help of bike commuters and the Los Angeles Bicycle Coalition. Using participatory design techniques such as visioning and scenario-based design, designers are working with bike commuters to design a participatory sensing system to improve bike commuting routes in Los Angeles. Bicyclists will contribute GPS data about their commutes, as well as images, tags, or other information about the route. Open design questions include the safest and most efficient ways to sense information about bike routes; the level of data sharing necessary to achieve useful project results; and protecting the privacy of participants' location traces.

Guideline III: Participant Autonomy

The goal of *participant autonomy* is building systems that enable participants to negotiate their own privacy concerns based upon preference and context. 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 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 of group decision-making.[40] After research groups have discussed default settings for discretion and sharing throughout the data life cycle, participants can take individual actions beyond the defaults to define their comfort with data collection and sharing according to situation, location, and culture. Individuals can also adjust for changing sensitivities and needs over time.

In order to take individual privacy-preserving actions, users will need to understand the data life cycle of a campaign, so that they can tailor capture, storage, sharing, and retention to their needs.

Mapping a Campaign

Mapping the data life cycle of a campaign can help to illustrate the campaign for participants and designers**.** Illustrating the privacy pressure points identified during the design process will help to identify the privacy decisions that need to be made by both participants and system designers. An example of a campaign mapping worksheet might look like this:

Campaign: X

Data Life Cycle	Participant Decision	Participant Action	Design Implication
1. Capture ↓	Participant decides when to enable capture.	Participant turns phone on/off or turns capture software on/off.	UI on phone to enable/disable capture.

[40] Margaret Cargo and Shawna L. Mercer, "The Value and Challenges of Participatory Research: Strengthening Its Practice," Annual Review of Public Health 29 (2008).

2. Storing ↓	Participant employs a pseudononymous username.	Participant registers a username that does not reveal identity.	Authentication system allows for pseudonyms as usernames.
	Participant decides to delete some captured data from their collection.	Participant views data via UI and elects to delete data.	UI and data store enable deletion of data at any granularity.
3. Processing ↓	Participant decides to be discrete with third party data.	Participant blurs, masks, declines to share, or deletes third party data.	UI allows easy masking, altering, and deleting.
4. Sharing ↓	Participant decides to share selected with designated people or processing programs.	Participant uses UI to select data for sharing, and to select desired recipients.	Data tore allows for feed customization, in-network sharing, or other selective sharing features.
5. Republishing ↓	Participant decides to alter data resolution before sharing to protect identity or confidentiality.	Participant uses UI to aggregate, limit or alter data to republish at a lower resolution.	UI and data store allow for resolution control. System also allows republishing.
6. Retention ↓	Participant decides their data should be deleted at the end of their campaign participation.	Participant uses UI to set generate metadata indicating internal retention period.	System complies with retention data through automatic deletion of 'expired' data.
	Participant monitors data shared with external applications.	Participant checks up on retention agreements with third parties by executing a hash.	System enables hash to compare data sets, monitor and negotiate with outside programs.
7. Reuse	Participant decides some of their data may be reused by future campaigns.	Participant uses UI to create reuse metadata.	System enables automatic enforcement of internal reuse policies.

Table 3: Campaign Mapping

Of course, the privacy protection decisions available to participants, and the system components needed to support those decisions, will vary on a campaign-by-campaign basis. Some of the considerations, justifications, and options for individual user control over each part of the data life cycle are discussed below.

Control Over Capture

Control over capture of data takes into account Palen & Dourish's *disclosure* and *identity* boundaries.[41] Individuals must have the ability to negotiate their own comfort level with publicity and disclosure, as well as how their identities as research participants mesh with other roles in their lives. Participants must also be able to understand what, exactly, they are capturing. CENS systems must be legible enough that participants understand what data is being captured, and what is not being captured.

Another privacy issue implicit in data capture is the problem of capturing data about third parties. Many CENS campaigns may capture data about third parties who are not participants in a research project. Examples would be images of fellow diners taken during a DietSense campaign, or images of strangers taken during a walkability campaign. Individuals not directly involved in a campaign will not have consented to data capture, and will not have any of the privacy controls allotted to campaign participants. Image-based campaigns are particularly vulnerable to capturing third party data.

One approach to protecting third parties from unwanted data capture is to alert them to data capture. Letting people know – either manually or automatically – that their image or voice is being recorded is considered good privacy practice, and several researchers have suggested ways of making capture systems visible to third parties.[42] This allows both participants and third parties to adjust their privacy expectations to fit the space of capture.[43] For example, Bellotti suggests considering the following design issues:[44]

Visibility & Perceptibility	• Data capture should be noticeable. • Notifications should give individuals opportunity to prevent or alter capture. • Participants should be able to learn the system's structure and cues easily.
Flexibility	• Participant should be able to stop or alter capture upon third party request. • Capture mechanisms should be lightweight to use and alter.
Unobtrusiveness	• Features such as notifications should not disrupt or annoy. • Visibility features should not compromise the privacy of participants.
Trustworthiness	• In order to instill confidence of privacy protections in both participants and third parties, the system and feedback must work as promised. • If participants take no action, data capture should be minimized.

[41] Palen and Dourish, "Unpacking "Privacy" For a Networked World."
[42] Victoria Bellotti, "Design for Privacy in Multimedia Computing and Communications Environments," Technology and Privacy: The New Landscape, eds. Philip E. Agre and Marc Rotenberg (Cambridge, MA and London: The MIT Press, 1998).
[43] Friedman, et al, "The Watcher and the Watched: Social Judgments About Privacy in a Public Place."; Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public."
[44] Bellotti, "Design for Privacy in Multimedia Computing and Communications Environments."

Notifying third parties of data capture may be difficult for some CENS campaigns. Ubiquitous computing applications have experimented with techniques for alerting third parties including signs, embedded screens, and drawing attention to recording equipment.[45] However, these applications were working within a designated space or environment: a room, a public plaza, etc. CENS urban sensing projects present the challenge of mobility. Because data capture can occur anywhere, notification mechanisms must be mobile. Ideas include wearing phones in use as cameras so that they are noticeable and obtrusive; or asking participants to inform third parties of data collection.

Drawing attention to data collection may have negative consequences as well, however. Drawing attention to the use of expensive instruments may invade participants' privacy or safety in some circumstances. And participants may forget to inform third parties of their data collection, particularly if it is occurring automatically throughout the day. CENS designers need to take the nature of the campaign into account when considering ways to protect the privacy of third parties.

Control Over Storage

User control over storage incorporates questions of authentication, access, retention and deletion. Must a user be identified in order to participate in a campaign (for instance, by entering their real name or through association with their Facebook profile or IMEI?) In any given campaign, who can access a user's raw and/or processed data? How should our systems authenticate access and track who has accessed the data?

Because different campaigns will have different requirements for user identity, data access, and sharing, CENS authentication and storage systems must be flexible enough to incorporate pseudononymous and anonymous identities; data sharing among restricted and customizable groups; and access tracking and notification.

Control Over Processing

Allowing users control over elements of data processing can provide a variety of privacy protections. For example, an image processing interface could allow participants to mask or delete images of third parties. Eventual control over processing could include participant ability to tailor the models through which data are fed to better fit their patterns and habits.

Control Over Sharing

Selective sharing is one of the most critical privacy controls a user can have. By defining who can see their data, when, and which data, participants can take advantage of the benefits of sharing while negotiating a comfortable space between disclosure and discretion.

[45] Friedman, et al, "The Watcher and the Watched: Social Judgments About Privacy in a Public Place."; Hayes, et al, "Physical, Social and Experiential Knowledge in Pervasive Computing Environments."; Victoria Bellotti and Abigail Sellen, "Design for Privacy in Ubiquitous Computing Environments," Third European Conf. Computer-Supported Cooperative Work ECSCW'93 (Milano, Italy: Dordrecht: Kluwer, 1993).

An ideal privacy-protecting system would default to making an individual's data available only to them. The participant could then customize data sharing by selecting specific data to share with chosen individuals, groups, or outside programs. Participants could also choose to represent their data at any granularity they wish. However, different campaigns will have different needs. Some campaigns may ask participants to agree to share all data with campaign organizers or participants. Some campaigns may share only *aggregate* data while keeping granular data private (see the PEIR design case study in the *Participatory Design* section.) CENS urban sensing systems must be customizable for all of these different selective sharing scenarios.

Another issue implicit in selective sharing is individual understanding of the risks and benefits of data sharing. Before a user agrees to share their data, they must understand what that data may indicate about their lives and habits. The connection between understanding data and sharing data further emphasizes the need for urban sensing data visualization and interfaces to make data legible and meaningful to even participants with little experience with data or technology.

Control Over Republishing

If data is to be shared or republished, CENS participants should be able to store or share aggregated or altered data to preserve confidentiality or to share data at a level of granularity with which they feel comfortable.

A National Research Council report discusses a variety of technical solutions for adjusting data resolution. These include:

- *data limitation* – restricting the number of variables, response values, or cases made available for sharing
- *data alteration* – swapping the attributes of respondents to reduce risk of identification, or masking data through perturbations or transformations of data points
- *secure access* – allowing participants access to the results of computations without allowing access to the data itself
- and *data simulation* – releasing synthetic data with similar characteristics to the genuine data.[46]

While each of these technical solutions has benefits for protecting privacy, each also has potentially negative consequences for data accuracy and analysis. CENS designers should work with campaign organizers to establish acceptable limits to user control over data representation and republishing.

Control Over Retention and Reuse

Negotiating the temporal boundaries of systems that collect personal information can be difficult.[47] Many systems that record personal data do not make retention periods obvious, and data is often kept indefinitely and reused for secondary purposes.[48] CENS argues that personal data collected for specific research purposes is best used primarily for those purposes.

---

[46] Panel on Confidentiality Issues Arising from the Integration of Remotely Sensed and Self-Identifying Data, Putting People on the Map: Protecting Confidentiality with Linked Social-Spatial Data, 48-58.
[47] Palen and Dourish, "Unpacking "Privacy" For a Networked World."
[48] Gordon Bell and Jim Gemmell, "A Digital Life," Scientific American March 2007; Yahoo.com, Yahoo! Privacy: Flickr, 2007, Available: http://info.yahoo.com/privacy/us/yahoo/flickr/details.html, November 13 2007.

Participants must be assured that their data will not be sold, distributed, or repurposed without their permission.

In order to give participants control over the retention of their data, several steps are needed. These include:

- Establishing clear and understandable, campaign-specific use guidelines for data.
- Establishing campaign-appropriate timelines for data retention and eventual deletion.
- Adjusting timelines and reuse policies at participant's request (for instance, participants could "donate" their data for future research.)
- Enabling system to append, track, and follow participant-selected retention and reuse metadata.
- Exploring data aggregation as a form of forgetting, fading of data over time.

There is a complex ethical debate surrounding the deletion of data that may have future reuse value, including future research value, historical value, or value as proof of integrity and accountability. Some archivists and researchers have set themselves against data destruction and in favor of data sharing.[49] Others argue that privacy should be protected in recordkeeping, even beyond basic legislative mandates.[50] Ketelaar, for example, espouses a participatory framework for understanding the privacy needs of archived data. He believes the more freedom a subject had in giving their data, and the more freedom they had to correct that data over time, the more access is ethically allowable to that data.[51]

Conversely, some researchers are now suggesting that the "forgetting" of data is in itself a positive social good.[52] Forgetting may allow for better regulation of personal identity over time, or social justice for groups (such as juvenile delinquents or those declaring bankruptcy) whose transgressions should be forgotten so that they may achieve a "clean slate".[53] Forgetting as a design principle may also lead to greater creativity in envisioning our relationship to data and data repositories.[54]

Feature Examples

Examples of design projects to encourage participant autonomy – user control over their own data – 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

[49] Tim Cook, "Archives and Privacy in a Wired World: The Impact of the Personal Information Act (Bill C-6) on Archives," Archivaria 53.Spring (2002).
[50] Eric Ketelaar, "The Right to Know, the Right to Forget?" The Archival Image: Collected Essays (Amsterdam: Hilversum, 1997).
[51] Ketelaar, "The Right to Know, the Right to Forget?"
[52] Bannon, "Forgetting as a Feature, Not a Bug: The Duality of Memory and Implications for Ubiquitous Computing"; Blanchette and Johnson, "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness."
[53] Blanchette and Johnson, "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness."
[54] Bannon, "Forgetting as a Feature, Not a Bug: The Duality of Memory and Implications for Ubiquitous Computing."

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.

Guideline IV: Minimal and Auditable Information

While the previous three guidelines are designed to facilitate CENS designers' interaction with sensing project participants, *minimal and auditable information* is addressed to CENS internal procedures for capturing, processing, storing, and reusing data. Minimal information implies targeted capture: by collecting only information relevant to given research objectives, CENS systems can contribute to innovative research while respecting participant privacy. Auditable information implies CENS responsibility for maintaining control over the data with which our systems are entrusted.

Minimal Information and Targeted Capture

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.

Suggestions for minimizing data capture include:

- Implement a campaign management framework that helps participants specify when, where, and what data will be collected.
- With the help of campaign organizers and/or participants, explicitly state the tradeoffs for each type of data captured.
- Utilize "right place right time" mechanisms: be sure that sensors only record data at agreed-upon places and times.
- Enable on-the-fly data deletion on the sensor itself, when possible.

Audit and Compliance

As the number of campaigns we conduct increases, CENS will become a warehouse for private data used by both participants and other researchers. Because of the quantities of data CENS will collect, we will need to deal with security, liability, and privacy issues. Auditing our information will allow us to keep our privacy promises to participants. Clearly defined audit procedures can help us ensure data access permissions, identify security and privacy breaches, and ensure compliance with user-specified retention and reuse policies.

The most important step for compliance may be having individuals who are responsible for ensuring audits happen. A good practice may be to designate someone from a campaign's development team whose explicit role is to follow up on privacy & participation issues throughout the entire data life cycle. The person in charge of data audits should be aided by a number of automatic mechanisms. Proper data provenance, access, reuse and retention metadata can facilitate automatic processes to share or delete data and alert the project team to breaches or problems in the system.

Future sharing of the data collected during urban sensing campaigns is another sensitive issue. A National Research Council report on protecting the confidentiality of participants gathering geospatial data recommends four basic policy levels of access to sensitive data:

- *full public access* for data files with little risk of exposure or harm;
- *limited licensing*, allowing other scientific institutions access, for data files that hold some risk of exposure or harm;
- *strong licensing*, requiring secondary institutions to get IRB approval before using the data, for data that exhibit a strong risk of disclosure;
- and *data enclaves*, access limited to within a research enclave, for data that present the greatest risk of exposure or harm.[55]

There are obvious trade-offs for participation and equity as the data is restricted through these levels. CENS might consider similar levels of restriction for secondary uses of campaign data, based upon the identifiability and exposure risk of the data and the participants' consent to data sharing.

Auditable information also encourages building strong privacy defaults during initial campaign development. Research has demonstrated that a majority of system users never change the privacy defaults of a system.[56] Minimal and auditable information encourages CENS to let users *opt in* to increased capture, sharing and long-term retention.

Feature Examples

System features that encourage minimal and auditable information include:

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.[57] Because participants must take explicit 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 that 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.

[55] Panel on Confidentiality Issues Arising from the Integration of Remotely Sensed and Self-Identifying Data, Putting People on the Map: Protecting Confidentiality with Linked Social-Spatial Data, 44-47.
[56] Waldo, et al, Engaging Privacy and Information Technology in a Digital Age.
[57] Hayes, et al, "Physical, Social and Experiential Knowledge in Pervasive Computing Environments."

Guideline V: Synergy between Policy and Technology

Software (or hardware, for that matter) cannot be the sole answer to ethical data collection and use.[58] System architecture will not be enough to ensure community participation or privacy safeguards. In a recent report on Privacy, the National Research Council recommends three tools for protecting privacy: individual actions, technology, and policy.[59] In order to meaningfully protect participant privacy, CENS must take advantage of all three.

Policy refers to guidelines to encourage participation or safeguard privacy. Policy can be agreed to at the institutional level (e.g. CENS policy), or at the campaign level (e.g. policy for PEIR). Examples of policy include:

- Campaign policy: the decision to capture only geospatial data during PEIR
- CENS policy: the decision to comply with participant-specified data retention dates

Policy is an important part of the research process: it can help research groups work through conflict and make decisions.[60]

Technical approaches to participation and privacy are design and architecture innovations that allow participants to meaningfully engage in campaigns. Examples of technological approaches to participation include:

- Participation: Designing usable and understandable systems for data capture and analysis
- Privacy: Designing systems to enable granular privacy decisions

Individual actions can be encouraged by both policy and system architecture. Individual actions allow participants choices in their privacy protection. Examples of individual actions include:

- Selective sharing of data
- Selective deletion of data

The National Research Council also recommends that if a system's design places the burden of protecting privacy on an individual, that systems support the individual in carrying this burden.[61] If CENS systems ask users to make complex privacy choices, we must support those choices by making them as intellectually understandable and logistically easy as possible.

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. 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.

---

[58] Waldo, et al, Engaging Privacy and Information Technology in a Digital Age.
[59] Ibid.
[60] T. Kriplean, I. Beschastnikh, D. W. McDonald and S. A. Golder, "Community, Consensus, Coercion, Control: Cs*W or How Policy Mediates Mass Participation," 2007 International ACM conference on supporting group work (ACM, 2007).
[61] Waldo, et al, Engaging Privacy and Information Technology in a Digital Age.

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.

Planning participatory sensing campaigns will almost always require making technical and policy decisions and facilitating individual actions. These decisions should be documented in the process of planning a campaign. The following section discusses details of documenting campaigns.

Campaign Documentation, Internal Review Board (IRB) and Informed Consent

Documenting Campaigns

The first step in the campaign documentation process is the online CENS Human Subjects Research form. https://research.cens.ucla.edu/intranet/urban_sensing/data_collection/

This form is designed to get campaign organizers thinking, and documenting, the data collection which will take place during a given campaign. This form documents the procedures and risks of ongoing CENS campaigns; helps researchers decide whether IRB approval is necessary; and creates a repository of CENS urban sensing projects.

Complying with IRB requirements

UCLA Internal Review Board guidelines are based upon federal guidelines established and enforced for any research or educational institution that receives government money.[62] Standard guidelines are that any research project that involves collecting data about people in order to contribute to *generalizable knowledge* needs to be reviewed by UCLA's IRB. Investigators may also apply for an exemption from full review. Generally, researchers need to submit their research protocol along with an informed consent form and a full summary of the risks and benefits of the proposed research.

Detailed instructions for complying with IRB guidelines can be found on the website of UCLA's Office for the Protection of Research Subjects (OPRS): http://www.oprs.ucla.edu/. In particular, we recommend that all CENS investigators download the UCLA *Investigator's Manual* (http://www.oprs.ucla.edu/oprs/human/documents/pdf/investigator-manual.pdf) and complete the online course for human subjects research certification (http://www.oprs.ucla.edu/human/certification).

Informed Consent

Informed consent is an ongoing process shared by researchers and research subjects.[63] In traditional human subjects research, gaining informed consent involves composing a form listing the risks and benefits of a research project, to which the research subject agrees by signing.

However, informed consent can also be interpreted along a spectrum of engagement and understanding. For instance, in fully participatory research projects designed and implemented entirely by the participating community, informed consent may be almost indigenous to the research process. In top-down sensing research, meaningful communication of research policies and practices is needed for the informed consent of participants.

Research on the readability of consent forms used as documentation in many research settings has shown these forms to be too often difficult and cumbersome to understand.[64] It is important

[62] Office of the Secretary of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research (Department of Health, Education, and Welfare, 1979).
[63] Panel on Institutional Review Boards Surveys and Social Science Research, Protecting Participants and Facilitating Social and Behavioral Sciences Research.

that CENS researchers take the consent form seriously, but also ensure communication with users throughout a sensing project in order to be sure that participants fully understand the data flows, risks, and benefits of a sensing project.

[64] Panel on Institutional Review Boards Surveys and Social Science Research, Protecting Participants and Facilitating Social and Behavioral Sciences Research.

Conclusion

Possibility, Not Restriction

Participation in sensing projects is a process of being involved in decisions about research goals, research design, system design, data collection, and data analysis. A part of all of these decisions are complimentary decisions about privacy. This report has outlined a series of principles that can help guide the interaction between CENS designers, campaign participants, and the data we collect and curate. Because participants with different privacy needs and goals will be actively involved in CENS sensing projects, all CENS design and research should take the steps outlined above to decide upon levels of participation and subsequent privacy enhancements.

Though CENS projects will take into account all of the design principles for privacy listed above, we do not wish to build systems so restricted that no use can be made of them. We hope that the design principles discussed in this report will encourage participation, so that socially-trusted urban sensing systems can reach their considerable research potential.

References

Ackerman, Mark S., and Lorrie Cranor. "Privacy Critics: UI Components to Safeguard Users' Privacy." Conference on Human Factors in Computing Systems CHI'99. ACM Publications.

Acquisti, Alessandro, and Ralph Gross. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." Privacy Enhancing Technologies 2006.

Altman, Irwin. "Privacy Regulation: Culturally Universal or Culturally Specific?" Journal of Social Issues 33.3 (1977): 66-84.

Anthony, Denise, David Kotz, and Tristan Henderson. "Privacy in Location-Aware Computing Environments." Pervasive Computing 6.4 (2007): 64-72.

Bannon, Liam. "Forgetting as a Feature, Not a Bug: The Duality of Memory and Implications for Ubiquitous Computing." CoDesign 2.1 (2006): 3-15.

Bell, Gordon, and Jim Gemmell. "A Digital Life." Scientific American March 2007: 58-65.

Bellotti, Victoria. "Design for Privacy in Multimedia Computing and Communications Environments." Technology and Privacy: The New Landscape. Eds. Philip E. Agre and Marc Rotenberg. Cambridge, MA and London: The MIT Press, 1998. 63-98.

Bellotti, Victoria, and Abigail Sellen. "Design for Privacy in Ubiquitous Computing Environments." Third European Conf. Computer-Supported Cooperative Work ECSCW'93. Dordrecht: Kluwer.

Blanchette, J.-F., and D.G. Johnson. "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness." The Information Society 18.33-45 (2002).

Burkert, Herbert. "Privacy-Enhancing Technologies: Typology, Critique, Vision." Technology and Privacy: The New Landscape. Eds. Philip E. Agre and Marc Rotenberg. Cambridge, MA and London: The MIT Press, 1998. 125-42.

Byrne, E., and P. M. Alexander. "Questions of Ethics: Participatory Information Systems Research in Community Settings." SAICSIT (Cape Winelands, South Africa, 2006).

Capurro, Rafael. "Privacy. An Intercultural Perspective." Ethics and Information Technology 7 (2005): 37-47.

Cargo, Margaret, and Shawna L. Mercer. "The Value and Challenges of Participatory Research: Strengthening Its Practice." Annual Review of Public Health 29 (2008).

Cook, Tim. "Archives and Privacy in a Wired World: The Impact of the Personal Information Act (Bill C-6) on Archives." Archivaria 53.Spring (2002): 94-114.

Corburn, Jason. "Bringing Local Knowledge into Environmental Decision Making: Improving Urban Planning for Communities at Risk." Journal of Planning Education and Research 22 (2003): 120-33.

Dredger, S. M., et al. "Using Participatory Design to Develop (Public) Health Decision Support Systems through GIS." International Journal of Health Geographics 6.53 (2007): n.d.

Friedman, Batya, et al. "The Watcher and the Watched: Social Judgments About Privacy in a Public Place." Human-Computer Interaction 21 (2006): 235-72.

Hayes, Gillian R., et al. "Physical, Social and Experiential Knowledge in Pervasive Computing Environments." Pervasive Computing 6.4 (2007): 56-63.

Iachello, Giovanni, and Jason Hong. "End-User Privacy in Human-Computer Interaction." Foundations and Trends in Human-Computer Interaction 1.1 (2007): 1-137.

Jensen, Carlos, et al. STRAP: A Structured Analysis Framework for Privacy. Atlanta, GA: Georgia Institute of Technology, 2005.

Ketelaar, Eric. "The Right to Know, the Right to Forget?" The Archival Image: Collected Essays. Amsterdam: Hilversum, 1997. 27-34.
Kriplean, T., et al. "Community, Consensus, Coercion, Control: Cs*W or How Policy Mediates Mass Participation." 2007 International ACM Conference on Supporting Group Work. ACM.
Lange, Patricia G. "Publicly Private and Privately Public: Social Networking on Youtube." Journal of Computer-Mediated Communication 13.1 (2007): n.d.
Lederer, Scott, Jason I. Hong, and Anind K. Dey. "Personal Privacy through Understanding and Action: Five Pitfalls for Designers." Pers Ubiquit Comput 8.November (2004): 440–54.
Muller, M. J. "Participatory Design: The Third Space in HCI." Handbook of HCI. Mahway, NJ: Erlbaum, 2003.
Nguyen, David H., and Elizabeth D. Mynatt. Privacy Mirrors: Understanding and Shaping Socio-Technical Ubiquitous Computing Systems: Georgia Institute of Technology, 2002.
Nissenbaum, H. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." Law and Philosophy 17.5-6 (1998): 559-96.
Nissenbaum, Helen. "Privacy as Contextual Integrity." Washington Law Review 79.1 (2004): 119–58.
Office of the Secretary of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research: Department of Health, Education, and Welfare, 1979.
Palen, Leysia, and Paul Dourish. "Unpacking "Privacy" For a Networked World." CHI 2003. ACM.
Panel on Confidentiality Issues Arising from the Integration of Remotely Sensed and Self-Identifying Data. Putting People on the Map: Protecting Confidentiality with Linked Social-Spatial Data. Washington, DC: National Research Council, 2007.
Panel on Institutional Review Boards Surveys and Social Science Research. Protecting Participants and Facilitating Social and Behavioral Sciences Research. Washington, DC: National Research Council, 2003.
Patil, Sameer, and Jennifer Lai. "Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application." SIGCHI Conf. Human Factors in Computing Systems (CHI 05). ACM Press.
Rambaldi, Giacomo, et al. "Practical Ethics for PGIS Practitioners, Facilitators, Technology Intermediaries and Researchers." Participatory Learning and Action 54.April (2006): 106-13.
Schuler, Doug, and A. Namioka. Participatory Design: Principles and Practices. Hillsdale, NJ: Lawrence Erlbaum Associates, 1993.
Waldo, James, Herbert S. Lin, and Lynette I. Millett. Engaging Privacy and Information Technology in a Digital Age. Washington, D.C.: The National Academies Press, 2007.
Yahoo.com. "Yahoo! Privacy: Flickr". 2007. Website. November 13 2007. <http://info.yahoo.com/privacy/us/yahoo/flickr/details.html>.