



Ethical Issues in Participatory Sensing

Katie Shilton and Deborah Estrin

Abstract

This article outlines the diverse ethical challenges embodied in participatory sensing, a form of data collection that allows individuals and groups to take advantage of pervasive mobile devices. These always-on, always-present devices carried by billions can capture and transmit users' location, images, motion, and user input. Mobile technologies are becoming a platform to document community needs and advocate for civic change, to understand personal habits and routines, and to document health problems and manage chronic illness. These new forms of data collection software utilize techniques traditionally employed by tools of surveillance: granular data gathering, sophisticated modeling, and inferences about personal behavior and attributes. Values such as privacy, consent, equity, and social forgetting are particularly challenged by this new form of data collection. The article draws from a three-year education project in a participatory sensing design laboratory to provide examples of ways to navigate these challenges through changes to design practice and ethics education.

Introduction

Emerging technologies enable individuals and communities to collect and share granular, accurate data about their lives and environments. These data are contributing to new treatments in health and wellness, discoveries in public health and social science, and community building and civic engagement. But they are also quite personal and sometimes sensitive; these technologies raise challenges to privacy, consent, and equity. They also challenge us to consider what data should be remembered and retained, or discarded and forgotten.

Consider, for example, a young man who is struggling to find a treatment plan for his depression. He believes his current medication dose is ineffective, but his doctor tells him his lack of progress is due to poor sleeping habits and medication nonadherence. The patient begins a self-monitoring program which generates new traces of his daily activities, sleep patterns, and medicine adherence. The phone records a combination of GPS and accelerometer readings to compare his daily activity levels. The device learns the time he wakes up and sends him a sleep quality survey. It also sends medication reminders at the proper time of day, and allows him to enter assertions that he's taken the medication. The phone sends all of this data—a record of his locations throughout the day as well as sensitive information about his health—to a server to draw inferences requested by the doctor or the patient, and guide discussions with his doctor and adjustments to his care plan.

A very different example is a mixed-income community in Los Angeles planning a community revitalization project. Community organizers help residents download software on their mobile phones. With the user's permission, the phones record GPS traces to document participants' routes to school and work. The phones also use location-based surveys to ask residents about the availability of healthy eating options, gathering places for youth, as well as less desirable aspects of the community like safety hazards and poor housing conditions. At the end of the data collection period, the community group uses annotated maps of community members' daily routines to contribute to a healthy community plan.

These two examples, different in scope and domain but similar in impact, illustrate the emerging phenomenon of participatory sensing.

Defining Participatory Sensing

Participatory sensing is a form of data collection that engages individuals in collecting data about themselves and their communities using digital devices. Participatory sensing is one of a number of related movements going under names including self-quantification, mobile health, bio-hacking, and self-surveillance (Dembofsky, 2011; Estrin & Sim, 2010; Hill, 2011).

Participatory refers to the way that this data collection proceeds: by engaging the consent and active participation of individuals and groups. *Sensing* refers to the use of software running on pervasive digital technologies such as mobile telephones which automatically log measurements like motion, location, and sound or images. In a broader use of the term, sensing also refers to the inference of an individuals' state from experience sampling streams and other mobile phone application usage, ranging from tweets to special health-related tools.

Ubiquitous digital tools are increasingly enabling individuals to collect very granular data about their habits, routines, and environments. Although forms of self-tracking have always existed, ubiquitous technologies such as the mobile phone enable a new scope and scale for these activities. These always-on, always-present devices carried by billions can capture and transmit users' location, images, motion, and text input. Technologists and engineers involved in participatory sensing endeavor to make these everyday devices a platform for coordinated investigation of the environment (Dutta et al., 2009; Mun et al., 2009) and human activity (Campbell, Eisenman, Lane, Miluzzo, & Peterson, 2006; Estrin & Sim, 2010; Froehlich, Chen, Consolvo, Harrison, & Landay, 2007; Miluzzo, Lane, Eisenman, & Campbell, 2007; Ramanathan, Swendeman, Comulada, Estrin, & Rotheram-Borus, 2011). Researchers are introducing these technologies into the public realm, a move that anticipates sensing by people across the world.

Pervasive mobile technologies harness the power of an existing platform—a distributed and ubiquitous network of mobile phones—for social projects. Users might benefit from phone location awareness to understand their exposure to air pollution as they move through a city. Communities could band together to undertake research projects using tools with which they are already familiar. Teams might use their phones to snap, tag, and upload photos of community events, perform volunteer assessments of the pedestrian or bike friendliness of neighborhoods, or to improve the ease of reporting environmental threats. Participatory sensing developers draw scenarios from community organizing and environmental justice, and imagine these tools deployed in public interest initiatives. Such powerful, familiar, and

plentiful sensors could enable interest groups to make their case through distributed documentation of problems, needs, or community assets.

Participatory sensing can take many forms, from personal investigation to coordinated research with many participants. For example, *Your Flowing Data*¹ is a project that asks individuals to send short messages recording data points (e.g., weight, exercise accomplished, mood, or food eaten) throughout the day. The project provides users with visualizations to explore patterns and learn from their data. A different example is *Ohmage* (Hicks et al., 2011), a mobile health application that combines location awareness with surveys about symptoms and habits, and mobility data. As with the young man struggling with depression described above, *Ohmage* helps participants work with a clinician or therapist to document behaviors and activities, such as sleep quality, stress, eating habits, or risk behaviors, as well as places and times when those behaviors are triggered. Depending on the needs of the study or the participant, *Ohmage* prompts users to input “experience samples” throughout the day (Csikszentmihalyi & Larson, 1987). These experience samples ask users to sample and record elements of their experience, such as feelings of stress or trouble sleeping, in real time. Experience samples might be triggered by a location (e.g., a bar or fast food restaurant) or time of day (e.g., upon waking). After a week of tracking and data analysis, users can see their experiences mapped to places and time, and work with their doctor to plan interventions.

Ethical Issues in Participatory Sensing

There are a plethora of social challenges introduced by the idea of collecting data about individuals using their mobile phones. While mobile data collection is both new and close to individuals, it invokes many of the same concerns posed by other forms of personal data collection: analysis of web use statistics by online marketers, warehousing of credit and retail information by data brokers, sharing of electronic medical records with insurers or employers, and tracking of location data by mobile phone providers and governments. Collections of personal data have wide potential for innovation and new knowledge creation, but they can also be invasive. These systems of mass personal data collection could also contribute to

¹ <http://yourflowingdata.com>

pervasive, ever-expanding surveillance systems. Corporations and governments find it strategically essential to inventory the world's information, compiling massive databases on people and their actions (Steel, 2010; Thurm & Kane, 2010). Participatory sensing, with its simultaneous prosocial potential and similarities to surveillance, serves as a complex case study into the shifting line between personal data collection and surveillance.

We describe four specific ethical issues that stem from concerns about surveillance: privacy, consent, equity, and social forgetting. These values spring from the academic literature on surveillance as well as study of values concerns in practice during participatory sensing design. Privacy is often defined as control over personal information. Consent is informed permission given to participate in data collection. Equity focuses on fairness and justice in how individuals are treated. Social forgetting is the purposeful discarding of information about individuals in order to enable forgiveness, recovery, or a clean slate. These values are not an exhaustive list; the challenges we have raised here are not the only ones suggested by participatory sensing. Values as diverse as sustainability, accessibility, openness, data literacy, and creativity are all relevant to participatory sensing. But because the social concern of surveillance is so specifically invoked by the data collection tools that facilitate participatory sensing, we focused on values meant to counter the pernicious effects of surveillance. Privacy, consent, equity and social forgetting are all tied to questions of surveillance, and are important social values regularly engaged by scholars in science and technology studies, information ethics, and participatory research ethics (Blanchette & Johnson, 2002; Lievrouw & Farb, 2003; Marx, 1998).

Focusing on privacy, consent, equity, and social forgetting also balances a blend of ethical frameworks. Privacy and social forgetting, values which emphasize protecting, obscuring or discarding sensitive data, are traditionally considered to be *utilitarian* ethics: focused on balancing costs and benefits of particular actions (Ess, 2009). A utilitarian framework tries to pursue acts that bring about the greatest number of positive consequences for the most number of people (Johnson, 2000). Privacy and social forgetting both focus on consequences: they are assumed (by theoreticians such as Marx, above) to ensure consequences that lead to

greater happiness. Conversely, values such as consent and equity emerge from *deontological* ethics, as articulated by philosophers such as Kant (Ess, 2009). Deontological ethics hold that some universal principles are inherent and inviolate. Deontological ethics are at the heart of human rights such as equity and human dignity; consent and equity are often seen as instrumental in the pursuit of human dignity.

Privacy

Using participatory sensing tools, individuals may gather data on their locations, health behaviors or symptoms, moods, eating or sleep. Such data can be incredibly revealing of individuals' habits, routines, and decisions (Christin, Reinhardt, Kanhere, & Hollick, 2011; Clarke, 2008; Krumm, 2007). Individuals have a range of willingness to share such data with family, friends, clinicians, or corporations, depending on both personal preference (Iachello, Smith, Consolvo, Chen, & Abowd, 2005; John, Acquisti, & Loewenstein, 2009; Tsai et al., 2009) and social context (Nissenbaum, 2009). With no specific legal protections for participatory sensing data, comprehensive databases documenting individuals' movements are prime targets for subpoena (Agre, 1998), and may even be demanded by U.S. authorities without warrant under the Patriot Act (Waldo, Lin, & Millett, 2007). In addition to seizure, risks of unauthorized sharing or data theft can occur at a variety of places in the design process. Small-scale application developers may not be able to follow best practice security, leaving data vulnerable to hackers or thieves (Zittrain, 2008). Complicated end-user licensing agreements may lead sensing participants to give away broad rights to share their data in return for services (Waldo et al., 2007). All of these concerns highlight a major challenge for participatory sensing: ensuring *privacy* for participants.

Privacy regulation and protection are critical topics in the design of ubiquitous and pervasive systems (Anthony, Kotz, & Henderson, 2007; Hayes et al., 2007; Hong & Satyanarayanan, 2007; Joseph, 2007; Surie, Perrig, Satyanarayanan, & Farber, 2007). There are also rich literatures on approaches to privacy in computer science and engineering, policy, law, and ethics. Computer science and engineering research innovates methods to obscure, hide, or anonymize data in order to give users privacy options (Ackerman & Cranor, 1999; Agrawal &

Srikant, 2000; Fienberg, 2006; Frikken & Atallah, 2004; Ganti, Pham, Tsai, & Abdelzaher, 2008; Iachello & Hong, 2007). Human-computer interaction research considers ways that systems might notify or interact with users to help them understand privacy risks (Anthony et al., 2007; Bellotti, 1998; Nguyen & Mynatt, 2002). Policy and legal research frame new regulations that could encourage individual and social privacy (Cohen, 2008; Kang, Shilton, Burke, Estrin, & Hansen, 2012; Nissenbaum, 2004; Waldo et al., 2007).

All of this cross-disciplinary attention points to the fact that *building systems* that protect privacy remains a challenge. Systems designed to protect privacy, often called Privacy Enhancing Technologies (PETs), have a mixed legacy (Burkert, 1998; Goldberg, 2008; Phillips, 2004). While PETs increase attention to privacy in both technical and social realms, their limitations are very real. PETs often can protect a single user from a more powerful organization but do not deal well with peer-to-peer data sharing, where sharing decisions may be fluid and changing. PETs also follow strict definitions of identifying information (for example, a person's name or social security number) and do not grapple with difficult concepts such as location privacy, in which identity may be implied from geo-location data (Burkert, 1998). Finally, PETs reify constrictive definitions of privacy, restricting privacy to controlling release of personally identifying data without recognizing fluid identities or contexts (Phillips, 2004).

Privacy, of course, is only a relative value, and can frustrate other social goods. As Kang (1998) points out, commerce can suffer from strong privacy rights, as there is less information for both producers and consumers in the marketplace. Perhaps worse, truthfulness, openness, and accountability can suffer at the hands of strict privacy protections (Allen, 2003). Participatory sensing research directly confronts this tradeoff between privacy, truthfulness, and accuracy. For example, researchers are developing algorithms for participatory sensing that allow users to replace sensitive location data with believable but fake data, effectively lying within the system (Ganti et al., 2008; Mun et al., 2009). What is good for privacy may not always be good for accuracy or accountability.

Consent

Privacy is not the only surveillance challenge raised by participatory sensing. Consent is a value central to research ethics in the United States, which have traditionally relied on federal guidelines such as the Belmont Report (Office of the Secretary of The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979) and Title 45 Code of Federal Regulations, Part 46 (Office for Protection of Research Subjects, 2007). These codes emphasize respect for human subjects, beneficence, and justice. A critical component of respect, beneficence and justice is informed consent.

Consent in participatory sensing, however, is complicated by relying on ubiquitous devices such as mobile phones: opting out of the mobile phone network is not a realistic option. Consent was at issue in the 2011 dust-up over Apple and Android location tracking, when it was revealed that both companies were storing location data over and beyond what users were notified of and consented to (Cheng, 2011; Markey, 2011).

Consent is further challenged by data use and sharing. Developers of location-based technologies may have financial motives to mine personal data, producing targeted advertising, selling valuable behavioral data to third parties, or using location to hone price or product discrimination (Curry, Phillips, & Regan, 2004). Even designers with excellent security practices and without a financial motive to mine the data may face challenges with large social repercussions. A design culture that encourages maximum data collection and retention, without consideration for targeting, focus or deletion, risks creating databases ripe for *function creep*: using amassed personal data for secondary, unforeseen purposes to which data subjects have not consented (Agre, 1994).

Researchers such as Gary Marx give examples of the ways that situational or structural factors weaken ideals of consent (Marx, 2006). Marx points out that law enforcement, government agencies, airport security, and other agents of power increasingly use "soft" surveillance techniques to collect seemingly voluntary but actually compelled data from individuals. Examples include searches to enter planes or subways (voluntary, but individuals may not ride

the transport if they do not volunteer), and withheld benefits by the Social Security Administration for parties who do not “voluntarily” submit personal information. Participatory sensing systems are one example of what could easily become a soft surveillance system. Because ubiquitous, networked sensors enable data collection in all spaces and places of users’ lives, they imply continuous participation of people either in or with the system. People can be involved in the system simply by agreeing to collect data. Such consent is fairly passive and may even be construed as soft surveillance if compelled by incentives or punishments.

While the Belmont Report and 45 CFR 46 provide excellent ethical starting points for participatory sensing research, the granularity, personal proximity, and participatory nature of sensing complicate notions of informed consent. For research systems that reside so close to individuals and collect such personal data, participation in data collection and analysis might be a stronger form of consent. In order to build systems that collect both meaningful and ethical data, systems must go beyond passive consent and encourage people to engage with them. This means that participants make decisions about system use or, in some scenarios, even design (Byrne & Alexander, 2006). Empowering users to participate in decisions about data collection, analysis, and research results preserves individual autonomy while interacting with otherwise invasive capture technologies.

Social forgetting

Always-on, sensitive data collection brings up a number of theoretical and normative issues related to whether and how this data should persist over time. The implications of creating a persistent record of people’s movements, habits, and routines are largely unexplored (Green, 2009, p. 267). Historically, archives focused on throwing records away, keeping only a tiny portion of records deemed historically valuable (Boles, 1991; Cook, 1991). But the explosion of data generation, paired with cheap storage and cloud computing, raises the possibility of saving much more evidence of daily life. This possibility has become a subject of both celebration (Bell & Gemmell, 2007) and debate (Blanchette & Johnson, 2002).

The ability to record everything and save it indefinitely to supplement fallible human memories is intriguing and perhaps even empowering. Limitless personal and community archives promise everything from improved health care (Hayes et al., 2007, 2008) to memory banks that “allow one to vividly relive an event with sounds and images, enhancing personal reflection” (Bell & Gemmell, 2007, p. 58). But as more data is collected and retained indefinitely, we must consider pernicious social consequences as well. Blanchette & Johnson (2002) point out that U.S. law has instituted a number of social structures to aid in *social forgetting*, or enabling a clean slate. These include bankruptcy law, credit reports and the clearing of records of juvenile offenders. As information systems increasingly banish forgetting, we may face the unintended loss of the fresh start. Dodge & Kitchin (2007) similarly worry that the phenomena like life-logging will engender total accountability for one’s actions, increased surveillance in the home and workplace, and the automatic sorting of people into commercial and social categories. Drawing on these arguments, Bannon (2006) suggests that building systems that forget might encourage new forms of creativity. He argues that an emphasis on augmenting one human capacity, memory, has obscured an equally important capacity: that of forgetting. He proposes that designers think about ways that sensing and other information systems might serve as “forgetting support technologies” (2006, p. 5). Mayer-Schoenberger (2007) presents a similar argument, advocating for a combination of policies and forgetful technologies that would allow for the gradual decay of digital data. Of course, purposeful decay of data would raise its own set of ethical issues around power, decision-making, and free speech. The ethics of social forgetting, framed as a proposed “right to be forgotten,” is currently under debate in the European Union (Rosen, 2012). The ways in which participatory sensing engineers and project organizers attend to data retention and forgetting will affect the social impacts and consequences of such data collections.

Equity

A focus on participation as a value for participatory sensing also suggests that questions of equity, power, and control undergird participatory sensing. Accumulating and manipulating information is a form of power in a global information economy (Castells, 1999; Lievrouw &

Farb, 2003). The individuals, institutions or corporations that instigate participatory sensing projects can control data collection, analysis, and presentation. Their goals will shape the kind of data collected and what conclusions are drawn about the data subjects. These groups may also decide who owns the data or benefits from sensing. How do participatory sensing stakeholders, such as designers, clients, and users, decide in whose hands this power will reside?

It is control that separates surveillance from other information systems (Lyon, 2001), and control is the pivot on which the question of participatory sensing technologies as surveillance turns. If powerful institutions gather data from relatively less powerful individuals, participatory sensing could tilt towards control and increased surveillance. The young man tracking his sleep and medication adherence might be required by his insurance company to document compliance with his doctor's orders. Alternatively, distributed sensing and analysis could shape technologies of care or even empowerment. The same young man might be free to experiment with his own regimens, or more experimental therapies suggested by his doctor. At the same time, the global availability of mobile phones provides an opportunity to radically lower the marginal cost of systematic data collection. Such availability could increase the accessibility of data-driven case-making to small institutions and community groups (Burke et al., 2006). These examples suggest that there is a spectrum along which the outcomes of sensing initiatives might be caring or controlling.

Incorporating Ethics into Design

Training engineering students and mobile developers to recognize the shifting and permeable boundary between data collection for individual or social goals, and corporate or government surveillance, is a challenging but important goal. With few existing legal protections for participatory sensing data, engineers and developers are primarily responsible for deciding how consent is handled, at what granularity data is collected, what conclusions are drawn from processed data, and for how long that data is retained. Participatory sensing is a prime

example of a design space in which ethical questions are matters of design. How can computer science and engineering students and participatory sensing designers pay attention and respond to these difficult social challenges as part of their design practice?

Values levers: Surfacing social values in design

Three years of participant-observation in a design laboratory has built a strong case study in the kinds of design practices that can help students attend to social values as part of their design work. This ethnographic project investigated how, as Verbeek (2006, p. 369) describes it, engineers “do ethics by other means.” Katie Shilton worked for three years an ethnographer within the Center for Embedded Networked Sensing (CENS), a science and technology research center lead by Deborah Estrin and based at the University of California, Los Angeles (UCLA). Shilton drew upon interviews, document analysis, and participant observation to learn how values like privacy, consent, equity, and social forgetting intersected with design work in this lab. Cooperating with Estrin and the other laboratory leaders as well as almost 30 students, Shilton analyzed interviews, meeting transcripts, and field notes taken during long stints in the lab for expressions of ideology, the justifications for those expressions, and the practices which triggered those expressions.

Coding this ethnographic data revealed that values tended to arise for discussion during a variety of design activities. These activities, which we identified as *values levers*, raised new conversations about ethics and values. Values levers are practices that pry open opportunities for discussion of antisurveillance values during design and helped build consensus around those values as design criteria. Four design practices in particular—experiencing internal testing, working on interdisciplinary teams, advocacy by a team member dedicated to values issues, and gaining funding—proved quite effective at generating consensus around, and technological features based on, antisurveillance values. One other, navigating the mandates of an outside ethics body (at UCLA, the Institutional Review Board), hold promise, but need adjustment to be truly powerful values levers.

Participating in prototype testing

Students reported discovering privacy, consent and equity concerns while testing prototypes of their applications and those of their colleagues. At CENS, as in many development labs, it was common practice to try new systems internally, before they were tested with users. The kinds of data under request (including location as well as questions about eating, sleeping and exercise habits) allowed students focus not only on the personal data collected, but the possible inferences that could be drawn from that data.

There is nothing novel about the finding that internal prototype testing is important to good design. However, the effects of such testing on designers' consideration of social values have gone unexplored. Prototype testing fostered a focus on personal data that was distinctive within the design process. When CENS students ran their colleagues' location-tracking programs over the weekend, or answered sensitive survey questions, they gained new respect for privacy and equity as design criteria. A practice meant to check new products for usability and bugs had the unanticipated result of making values personal and encouraging researchers to reflect on the sensitivity of the personal data in their systems.

Participating in interdisciplinary teams

Working alongside colleagues from other disciplines was another design practice that encouraged a focus on personal data, leading to discussions of privacy, consent, equity and social forgetting. The majority of CENS participatory sensing designers had undergraduate degrees in computer science (CS) or electrical engineering (EE). However, a small but vocal number of the design team hailed from statistics, design/media arts, and information studies. Statisticians, for example, attended weekly meetings and were a regular part of design. Their needs were almost as primary to the design process as those of the computer scientists.

Statisticians' comments and interests during design meetings frequently referred designers back to issues inherent in the data. This refocusing on project data was the (largely unintentional) deployment of a values lever. It allowed for not only statistical discussions, but

also ethical debate about data representation, sharing, and security. The unusually interdisciplinary nature of CENS design positioned the data collected by participatory sensing as a bridge between computer science, statistics, design/media arts, and information studies. Being forced to talk across disciplinary boundaries helped the design team articulate social values of importance.

Internalizing team member advocacy

As a values advocate and researcher hired to explicitly consider values issues in design, Shilton engaged in a number of activities that helped to deploy values levers. During high-level design meetings, specific advocacy was a useful tool. Shilton raised issues of privacy, consent, equity and social forgetting in group meetings, where the large and often interdisciplinary groups meant systems were discussed at the relatively high level. Shilton also worked with students on the more specific, lower-level details of design. This often took the form of working one-on-one with a student wrestling with a particular system implementation.

While Shilton's presence seemed to normalize the discussion of antisurveillance values, it also helped move responsibility for those design decisions away from engineers. Further longitudinal study may be necessary to determine if CENS designers engage antisurveillance values in future research when there is not a values advocate involved in design work.

Gaining funding

Resources and funding were also values levers at CENS, as they encouraged practices that fostered attention to values. Funding greatly affected the trajectory of projects. Funding guaranteed graduate students to work on a project, full-time staff to concentrate on duties unwanted by or unsuited to graduate students, and resources such as phones and server space to devote to a project. Larger, better funded CENS projects had correspondingly large development teams. Large teams required formal weekly planning meetings and fairly clear lines of communication. Antisurveillance values tended to come up in these meetings, due to a variety of factors. CENS leaders were often in these meetings, as was values advocate Shilton. In addition, the discussions fostered by a larger group of people tended to reveal social worries and opinions, which then become design concerns.

The design of larger systems contrasted to smaller projects, which had little or no initial funding and only two or three students focused on development part-time. Design meetings for these projects were informal and often spur-of-the-moment. Leaders and team members communicated about these projects largely over email. These less complex systems, which harbored less obviously sensitive personal data, were perceived to need less planning in advance. And fewer ethical concerns surfaced in the discussions of the small working teams.

Navigating institutional mandates

Values levers were often deployed by people close to design, including colleagues from statistics, as well as leaders and mentors. But CENS designers were also influenced by agents farther from design, including administrators responsible for the responsible conduct of research at UCLA. The university imposed its own ethical mandates on CENS design, enforced through the oversight of the Institutional Review Board (IRB), which was set up to monitor research ethics at UCLA.

CENS leaders were proactive about approaching the IRB, and actively informed it of research developments. The IRB was, in turn, flexible and accommodating of CENS timelines and internal procedures. The IRB considered most CENS projects to be technical pilots or services, rather than human subjects research, because the project data was not used to draw generalizable conclusions about human behavior. Only a handful of CENS projects qualified for review by the IRB, and most of those received an Exempt status from the board. But though it was an infrequent requirement, and though the IRB demonstrated real willingness to work with CENS engineers, designers considered seeking IRB approval to be undesirable or even painful, because it required paperwork, could take quite a bit of time, and therefore slowed down the pace of testing and implementation. The focus on paperwork made IRB discussions into administrative tasks, rather than central to design decision-making. The IRB served as a hurdle to be cleared, and students offloaded much of the required writing to a staff member hired to interface with the IRB. In this way, the IRB functioned very differently than other values levers, which brought values discussions into design meetings. The IRB's intervention

at CENS served as a values lever, helping to normalize and routinize values in much the same way as laboratory procedures imposed by leaders. It is unclear, however, how much impact this lever had on design. The combination of outsider status and perceived lack of understanding frustrated the IRB's effectiveness.

Best practices for ethics education in the lab

Values levers in design suggest a series of best practices for structuring the design laboratory and can help developers launching participatory sensing projects implement appropriate standards for data protection and privacy, consent, data retention and forgetting, and equity. These practices can help structure design laboratories so that values levers can flourish.

Increase attention to personal data

Work practices at CENS that facilitated attention to the sensitive data collected in participatory sensing, its meanings, and its potential uses, encouraged antisurveillance values in design. Issues of privacy, consent, equity and social forgetting were intimately tied to contemplation of what kinds of data were being collected, who could access them, when and how they were shared, and how they could be interpreted. Talking about personal data, and the processes surrounding that data, tended to include talking about values. Prototype testing can also be a powerful tool for redirecting designer attention to the data. Rewarding students for testing their own software, and that of colleagues, can promote a design culture in which sensitive data is taken seriously. Good data management practices, such as descriptive metadata, secure storage, and reuse policies, may also be a part of attention to data (Borgman, Wallis, & Enyedy, 2007; Mayernik, Wallis, Borgman, & Pepe, 2007).

Encourage interdisciplinarity

Including statisticians and a social scientist in design at CENS provided a values lever by sparking conversations using the lingua franca of participatory sensing: personal data. Industrial laboratories have long known that interdisciplinarity can encourage good design; CENS provides a case study in which interdisciplinarity encouraged values in design. Interdisciplinarity is not only a matter of recruiting and hiring a diverse workforce, but also of

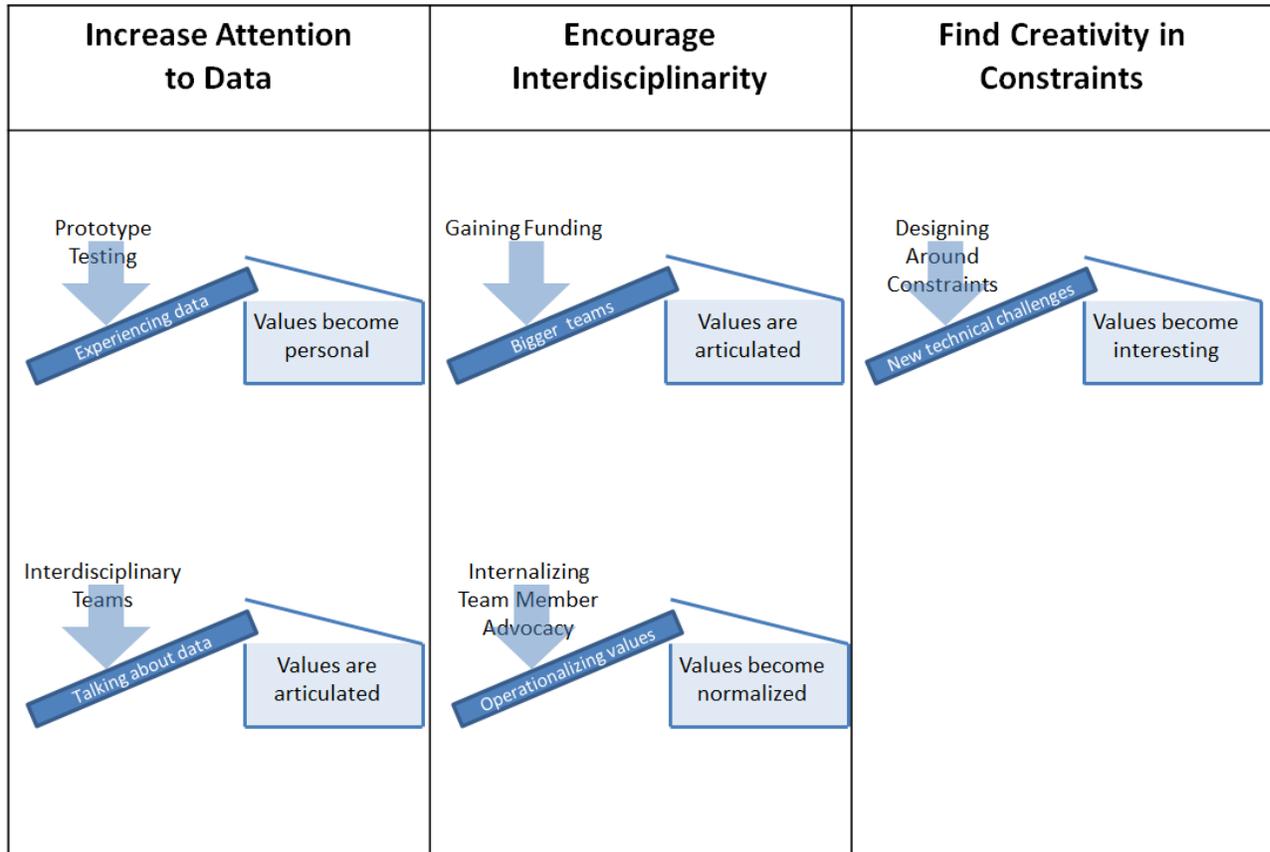
encouraging sometimes difficult cross-disciplinary conversations, and paying attention to uneven power dynamics between disciplines. Statisticians should be not just consultants brought in for data analysis, but full members of the design team. Social scientists must be welcomed as contributors although they may struggle to understand the intricacies of a system diagram. Giving social scientists, ethicists, or statisticians physical space in the laboratory is an important first step. Just as important is taking their contributions seriously and attempting to reach across lines of hierarchy and privilege by engaging material and perspectives from other disciplines. Reciprocation for this acceptance is also important: team members not actively writing software code must do work that contributes to the life of the laboratory. For social scientists trained in values concerns and information ethics, operationalizing values in design can be a critical design role. Helping design teams move from abstract values of importance, like privacy or equity, to technological features, was a process of translation well-suited for individuals trained in thinking about the sociotechnical nature of design. And such work contributed directly to design, making social values directly useful to design.

Finding the creativity in the constraints

Laboratories that incorporate user perspectives must allow for a slower design pace in order to foster this element of a critical technical practice. Similarly, it is important to embrace the slower design pace that values constraints sometimes impose on design. Though concerns such as privacy and consent may seem to slow down design progress, they also open spaces for new technical creativity. Recognizing that innovation sometimes comes from constraints is a design philosophy that laboratory leaders and values advocates can encourage on their teams.

These best practices, and the values levers they encourage, are summarized in **Figure 1** below.

Figure 1: Best Practices to Encourage Values Levers



Next Steps and Future Research

There are a number of unanswered questions in participatory sensing that require continued engagement between technology development and ethics. A continued focus on privacy requires the design and field testing of privacy-friendly participatory sensing systems. Researchers might conduct user studies to evaluate how participants understand and use their privacy choices, or study how combining multiple data collections might complicate privacy concerns. Researchers focused on access and equity can analyze the lines of power and participation in existing and emerging participatory sensing projects. They might collect demographic information on the populations participating in, and affected by, pervasive personal data projects, or interview stakeholders and understand the mix of organizational and informal publics involved in data collection projects. Researchers could question and critique

the usefulness of pervasive personal data, or they might establish guidelines for making data collection efforts truly participatory. And philosophical inquiry into memory and forgetting can help to answer the normative questions of what data should be actively curated, and what data are better left to digital obscurity. By querying and shaping how pervasive personal data are organized and managed; how privacy, consent, and participation are handled in pervasive systems; how pervasive personal data affects the balance of power in an information economy; and how such systems impact social and institutional memory and forgetting, ethicists and engineers can help to shape this emerging information landscape through building systems, constructing information policy, and shaping values in participatory sensing design.

References

- Ackerman, M.S., & Cranor, L.F. (1999). Privacy critics: UI components to safeguard users' privacy. *Conference on Human Factors in Computing Systems CHI'99* (pp. 258–259). ACM Publications.
- Agrawal, R., & Srikant, R. (2000). Privacy-preserving data mining. *2000 ACM SIGMOD International Conference on Management of Data* (pp. 439–450).
- Agre, P. E. (1994). Surveillance and capture: two models of privacy. *The Information Society*, *10*(2), 101–127.
- Agre, P.E. (1998). Beyond the mirror world: Privacy and the representational practices of computing. In Agre, P.E. & Rotenberg, M. (Eds.), *Technology and privacy: The new landscape* (pp. 29–61). Cambridge, MA and London: The MIT Press.
- Allen, A.L. (2003). *Why privacy isn't everything: feminist reflections on personal accountability*. Lanham, Boulder, New York and Oxford: Rowman & Littlefield Publishers, Inc.

- Anthony, D., Kotz, D., & Henderson, T. (2007). Privacy in location-aware computing environments. *Pervasive Computing*, 6(4), 64–72.
- Bannon, L. (2006). Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing. *CoDesign*, 2(1), 3–15.
- Bell, G., & Gemmell, J. (2007). A digital life. *Scientific American*, (March), 58–65.
- Bellotti, V. (1998). Design for privacy in multimedia computing and communications environments. In Agre, P.E. & Rotenberg, M. (Eds.), *Technology and privacy: The new landscape* (pp. 63–98). Cambridge, MA and London: The MIT Press.
- Blanchette, J.-F., & Johnson, D.G. (2002). Data retention and the panoptic society: the social benefits of forgetfulness. *The Information Society*, 18(33-45).
- Boles, F. (1991). *Archival Appraisal*. New York and London: Neal-Schuman Publishers, Inc.
- Borgman, C. L., Wallis, J. C., & Enyedy, N. (2007). Little science confronts the data deluge: habit ecology, embedded sensor networks, and digital libraries. *International Journal on Digital Libraries*, 7(1-2), 17–30.
- Burke, J., Estrin, D., Hansen, M., Parker, A., Ramanathan, N., Reddy, S., & Srivastava, M. B. (2006). *Participatory sensing*. *World Sensor Web Workshop*. Presented at the World Sensor Web Workshop, Boulder, CO: ACM.
- Burkert, H. (1998). Privacy-enhancing technologies: Typology, critique, vision. In Agre, P.E. & Rotenberg, M. (Eds.), *Technology and privacy: The new landscape* (pp. 125–142). Cambridge, MA and London: The MIT Press.
- Byrne, E., & Alexander, P. M. (2006). Questions of ethics: Participatory information systems research in community settings. *Proceedings of the 2006 annual research conference of*

the South African institute of computer scientists and information technologists on IT research in developing countries (pp. 117–126).

Campbell, A.T., Eisenman, S.B., Lane, N.D., Miluzzo, E., & Peterson, R.A. (2006). People-centric urban sensing. *Proceedings of the 2nd annual international workshop on Wireless internet*. Boston, MA: ACM.

Castells, M. (1999). Flows, networks, and identities: A critical theory of the informational society. In *Critical education in the new information age*. Lanham, MD: Rowman & Littlefield Publishers, Inc.

Cheng, J. (2011, April 21). How Apple tracks your location without consent, and why it matters. *ars technica* [Blog]. Retrieved from <http://arstechnica.com/apple/news/2011/04/how-apple-tracks-your-location-without-your-consent-and-why-it-matters.ars>

Christin, D., Reinhardt, A., Kanhere, S. S., & Hollick, M. (2011). A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software*, 84(11), 1928–1946.

Clarke, R. (2008). *You Are Where You've Been* (Working Paper). Xamax Consultancy Pty Ltd. Retrieved from <http://www.rogerclarke.com/DV/YAWYB-CWP.html>

Cohen, J.E. (2008). Privacy, visibility, transparency, and exposure. *University of Chicago Law Review*, 75(1), 181–201.

Cook, T. (1991). *The archival appraisal of records containing personal information: A RAMP study with guidelines*. Paris: General Information Programme, United Nations Educational, Scientific and Cultural Organization.

Csikszentmihalyi, M., & Larson, R. (1987). Validity and reliability of the Experience-sampling method. *The Journal of Nervous and Mental Disease*, 175(9), 526–536.

- Curry, M.R., Phillips, D.J., & Regan, P.M. (2004). Emergency response systems and the creeping legibility of people and places. *The Information Society*, 20, 357–369.
- Dembosky, A. (2011, June 10). Invasion of the body hackers. *FT Magazine*. Retrieved from <http://www.ft.com/cms/s/2/3ccb11a0-923b-11e0-9e00-00144feab49a.html#axzz1RxISmSku>
- Dodge, M., & Kitchin, R. (2007). "Outlines of a world coming into existence": pervasive computing and the ethics of forgetting. *Environment and Planning B: Planning and Design*, 34(3), 431–445.
- Dutta, P., Aoki, P. M., Kumar, N., Mainwaring, A., Myers, C., Willett, W., & Woodruff, A. (2009). Common Sense: participatory urban sensing using a network of handheld air quality monitors. *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, SenSys '09* (pp. 349–350). New York, NY, USA: ACM. doi: [10.1145/1644038.1644095](https://doi.org/10.1145/1644038.1644095)
- Ess, C. (2009). *Digital media ethics*. Cambridge, UK and Malden, MA: Polity Press.
- Estrin, D., & Sim, I. (2010). Open mHealth Architecture: An Engine for Health Care Innovation. *Science*, 330(6005), 759–760.
- Fienberg, S.E. (2006). Privacy and confidentiality in an e-commerce world: Data mining, data warehousing, matching and disclosure limitation. *Statistical Science*, 21(2), 143–154.
- Frikken, K.B., & Atallah, M. J. (2004). Privacy preserving route planning. *Proceedings of the 2004 ACM workshop on privacy in the electronic society* (pp. 8–15). Presented at the 2004 ACM workshop on Privacy in the electronic society, Washington DC, USA: ACM.

- Froehlich, J., Chen, M. Y., Consolvo, S., Harrison, B., & Landay, J.A. (2007). MyExperience: a system for in situ tracing and capturing of user feedback on mobile phones. *Proceedings of the 5th international conference on Mobile systems, applications and services, MobiSys '07* (pp. 57–70). New York, NY, USA: ACM.
- Ganti, R.K., Pham, N., Tsai, Y.-E., & Abdelzaher, T. F. (2008). PoolView: stream privacy for grassroots participatory sensing. *Proceedings of the 6th ACM conference on embedded network sensor systems* (pp. 281–294). Raleigh, NC, USA: ACM.
- Goldberg, I. (2008). Privacy-enhancing technologies for the Internet III: Ten years later. In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & Sabrina de Capitani di Vimercati (Eds.), *Digital privacy: Theory, technologies, and practices* (pp. 3–18). New York and London: Auerbach Publications.
- Green, N. (2009). Mobility, memory, and identity. In G. Goggin & L. Hjorth (Eds.), *Mobile technologies: from telecommunications to media* (pp. 266–281). New York and London: Routledge.
- Hayes, G. R., Abowd, G., Davis, J., Blount, M., Ebling, M., & Mynatt, E. (2008). Opportunities for Pervasive Computing in Chronic Cancer Care. *Pervasive Computing 2008* (pp. 262–279). Lecture Notes in Computer Science, Vol. 5013. Heidelberg: Springer-Verlag.
- Hayes, G. R., Poole, E. S., Iachello, G., Patel, S. N., Grimes, A., Abowd, G., & Truong, K. N. (2007). Physical, social and experiential knowledge in pervasive computing environments. *Pervasive Computing*, 6(4), 56–63.
- Hicks, J., Ramanathan, N., Falaki, H., Longstaff, B., Parameswaran, K., Monibi, M., Kim, D. H., et al. (2011). *Ohmage: an open mobility system for activity and experience sampling* [CENS Technical Report No. 100]. Los Angeles, CA: Center for Embedded Networked Sensing.

- Hill, K. (2011, February 25). Adventures in self-surveillance: Fitbit, Tracking My Movement and Sleep [Technology blog]. Forbes. Retrieved from <http://blogs.forbes.com/kashmirhill/2011/02/25/adventures-in-self-surveillance-fitbit-tracking-my-movement-and-sleep/>
- Hong, J., & Satyanarayanan, M. (2007). Security & privacy. *Pervasive Computing*, 6(4), 15–17.
- Iachello, G., & Hong, J. (2007). End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction*, 1(1), 1–137.
- Iachello, G., Smith, I., Consolvo, S., Chen, M., & Abowd, G. (2005). Developing privacy guidelines for social location disclosure applications and services. *Proceedings of the 2005 symposium on Usable privacy and security* (pp. 65–76). Pittsburgh, Pennsylvania: ACM.
- John, L. K., Acquisti, A., & Loewenstein, G. (2009). *The best of strangers: Context dependent willingness to divulge personal information* [Working Paper]. Pittsburgh, PA: Carnegie Mellon University. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1430482
- Johnson, D. G. (2000). *Computer Ethics* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.
- Joseph, A. D. (2007). Works in progress: security and privacy in pervasive computing. *Pervasive Computing*, 6(4), 73–75.
- Kang, J. (1998). Privacy in cyberspace transactions. *Stanford Law Review*, 50, 1193–1294.
- Kang, J., Shilton, K., Burke, J., Estrin, D., & Hansen, M. (2012). Self-surveillance privacy. *Iowa Law Review*, 97(3), 809–847.

- Krumm, J. (2007). Inference attacks on location tracks. *Proceedings of the 5th international conference on pervasive computing, PERVASIVE'07* (pp. 127–143). Berlin, Heidelberg: Springer-Verlag.
- Lievrouw, L. A., & Farb, S. E. (2003). Information and social equity. In Cronin, B. & Shaw, D. (Eds.), *Annual review of information science and technology, Volume 37* (pp. 499–540).
- Lyon, D. (2001). *Surveillance Society* (1st ed.). Buckingham and Philadelphia: Open University Press.
- Markey, E. (2011, April 21). Letter from Congressman Markey to Steve Jobs. Retrieved from http://markey.house.gov/docs/apple_ios_letter_04.21.11.pdf
- Marx, G. T. (1998). Ethics for the new surveillance. *The Information Society, 14*, 171–185.
- Marx, G. T. (2006). Soft surveillance: The growth of mandatory volunteerism in collecting personal information—“Hey Buddy Can You Spare a DNA?” In T. Monahan (Ed.), *Surveillance and Security: Technological Politics and Power in Everyday Life* (pp. 37–56). New York and London: Routledge.
- Mayernik, M. S., Wallis, J. C., Borgman, C. L., & Pepe, A. (2007). Adding context to content: The CENS deployment center. Presented at the *Annual Meeting of the American Society for Information Science & Technology*, Milwaukee, WI.
- Mayer-Schoenberger, V. (2007). *Useful void: the art of forgetting in the age of ubiquitous computing* [Working Paper No. RWP07-022]. Cambridge, MA: Harvard University.
- Miluzzo, E., Lane, N. D., Eisenman, S. B., & Campbell, A. T. (2007). CenceMe - Injecting sensing presence into social networking applications. In: *Smart Sensing and Context* (pp. 1-28). Lecture Notes in Computer Science, Vol. 4793.

- Mun, M., Reddy, S., Shilton, K., Yau, N., Boda, P., Burke, J., Estrin, D., et al. (2009). PEIR, the personal environmental impact report, as a platform for participatory sensing systems research. *Proceedings of the International Conference on Mobile Systems, Applications, and Services* (pp. 55–68). Presented at the International Conference on Mobile Systems, Applications, and Services, Krakow, Poland: ACM.
- Nguyen, D. H., & Mynatt, E. (2002). *Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems*. Georgia Institute of Technology.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119–158.
- Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford Law Books.
- Office for Protection of Research Subjects. (2007, March 30). *UCLA Investigator's Manual for the Protection of Human Subjects*. Retrieved from <http://www.oprs.ucla.edu/human/manual/TOC>
- Office of the Secretary of The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research*. U.S. Department of Health, Education, and Welfare.
- Phillips, D. J. (2004). Privacy policy and PETs: the influence of policy regimes on the development and social implications of privacy enhancing technologies. *New Media & Society*, 6(6), 691–706.
- Ramanathan, N., Swendeman, D., Comulada, S., Estrin, D., & Rotheram-Borus, M. J. (2011). *Identifying preferences for mobile health applications of self-monitoring and self-*

- management: focus group findings from HIV-positive persons and young mothers* [CENS Technical Report No. 101]. Los Angeles, CA: Center for Embedded Networked Sensing.
- Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online*, 64, 88.
- Steel, E. (2010, March 15). Exploring ways to build a better consumer profile. *The Wall Street Journal*. Retrieved from <http://online.wsj.com/article/SB10001424052748703447104575117972284656374.html>
- Surie, A., Perrig, A., Satyanarayanan, M., & Farber, D. J. (2007). Rapid trust establishment for pervasive personal computing. *Pervasive Computing*, 6(4), 24–30.
- Thurm, S., & Kane, Y. I. (2010, December 18). Your apps are watching you. *The Wall Street Journal*. Retrieved from <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html>
- Tsai, J. Y., Kelley, P., Drielsma, P., Cranor, L. F., Hong, J., & Sadeh, N. (2009). Who's viewed you?: the impact of feedback in a mobile location-sharing application. *Proceedings of the 27th international conference on Human factors in computing systems* (pp. 2003–2012). Boston, MA, USA: ACM.
- Verbeek, P.-P. (2006). Materializing morality. *Science, Technology & Human Values*, 31(3), 361–380.
- Waldo, J., Lin, H. S., & Millett, L. I. (2007). *Engaging privacy and information technology in a digital age*. Washington, D.C.: The National Academies Press.

Zittrain, J. (2008). *The future of the internet—And how to stop it*. New Haven & London: Yale University Press.

This article should be cited as:

Shilton, K & Estrin, D. (2012). Ethical issues in participatory sensing. *CORE Issues in Professional and Research Ethics*, 1(Paper 5).



ncpre

National Center for
Professional and
Research Ethics