Privacy Awareness for the Design of Pervasive Home-Based Technology for Elders

Tonya Thompson and Jean Camp

Abstract

In this paper, we discuss the importance and difficulty of defining privacy in a way that can usefully inform design. We then present existing conceptual models of privacy from previous work by researchers and designers. Of greatest relevance is the concept of privacy as contextual, which inextricably ties privacy to the needs and expectation of the user. Next, we illustrate privacy issues, using scenarios, in the context of in-home elder support. Finally, we describe a privacy-aware design model that demonstrates the application of a person-as-context approach to privacy to the design of pervasive home-based technology for elders. Ultimately, this model is meant to help the designer generate a set of questions that are to be used as a tool for giving the user an active role in the early stages of the design process. These questions create a dialogue between the designer and the user that enables the user to help construct the specifications of the privacy features of their home based technologies.

1. Intro: the Problem with Privacy

In the design of technology, there is no universal agreement on what privacy should look like. However, new threats to privacy call for an awareness of the privacy implications of design. In particular, home-based monitoring technology for an aging population that wants to remain independent and at home for as long as possible creates an increased need to protect information in private spaces. Given the dangers that come with the functionality of information gathering and storage technologies, privacy implications of pervasive technology must be considered when designing devices or systems for personal spaces. Although developers can create secure, privacy-preserving technologies, the expectations and behaviors of the end user will determine the effectiveness of security measures. A user experience designer must have an understanding of the privacy implications of the security of the technology and how use by the intended user group may compromise privacy-preserving features.

In order to adopt a “do no harm” approach [1] to pervasive technologies in the home, designers must have some way of designing with privacy awareness because loss of privacy can be financially, socially and psychologically damaging to users [2].

The problem is that the meaning of privacy is ambiguous and therefore hard to apply practically [3]. Privacy concepts are numerous and their implications are complex. Assumptions about privacy attitudes are wrong largely because privacy is not universally well defined [4]. This ambiguity reconciles the inconsistency between the increased level of concern people claim to have regarding privacy and their surprising willingness to reveal highly personal information in exchange for a reward of negligible value [5].

Designers, as well as researchers, have different concepts of privacy [6] and these notions become “embedded” in technology [7]. Once embedded, the privacy assumptions of the designer influence the lives of users, who have their own understanding of privacy. The attitudes and behaviors of a user, related to this understanding, will ultimately determine how the technology is used and how well the user’s privacy is preserved. Consequently, understanding the user’s concept of privacy is necessary in privacy aware design.

So, it is not only necessary to have a working definition of privacy, it is also necessary to be able to clearly communicate that definition to others in order to discuss and evaluate the privacy implications of design decisions [8]. Because design relies heavily upon prototype evaluation, a definition of privacy can only be effective and useful in design implementation if it fits into conceivable descriptions and realistic examples that are relevant to the designer [9].

As certain technology makes personal information increasingly difficult to protect, a persistent and significant effort has been made, in multiple disciplines, to find a manageable and practical definition of privacy of technology. However, one universal definition of "privacy for design" may not work when applied to diverse, evolving technologies intended for diverse, changeable populations. A working definition that allows for flexibility and modification seems most appropriate for designers. In reading previous research on this topic, we have identified some general conceptual frameworks of privacy that are relevant to the design process. Ultimately, we found that a contextual concept of privacy provides designers with a useful way to think about privacy implications of design. This concept allows the designer to understand privacy through user expectations of privacy, in terms of specific users and specific technologies.

1.1 Privacy as Rights

Privacy has been described as "rights against the world" [10]. A more elaborate description involves three dimensions: privacy as a human right, a right to seclusion and a property right [11].

As a human right of autonomy, privacy involves independent thought and action. In other words, people should have control over their own personal information. They should be able to do with it what they want. The right to dignity is a right to transparency of monitoring and use of shared information [12]. It means that two communicating parties should have the same amount of visibility of intention in a transaction.

As a right to seclusion, privacy is protected by freedom from hidden surveillance in areas of expected solitude. It also means that personal information can not be traced back to its owner [4].

This approach can also treat personal identifiers as a property that can be sold or traded. So, private information can be traded for services from Facebook, MySpace, amazon.com, or Google. In exchange for applications, customized content, and discounts, people have the ability to pay with their unique identifiers, such as name, age, gender, sexual orientation, religion, social security number, street address and phone number [13].

1.2 Privacy as Visibility

Privacy is essentially fair disclosure of information and effective visualization of information. In the first sense, visibility means that users are aware of what information they are sharing and how that information can be used [14]. In the case of visualization, privacy is a product of user understanding; more awareness leads to better protection of private information through secure systems. Although security is not privacy, in order for information to be private it must also be secure [15]. Poor visibility features of technology cause the practical level of security to consistently falling below predicted levels. This is a visualization problem that can be solved by the "visible security approach", which allows users to understand the behaviors of technology related to their daily computing activities [16]. People make mistakes, or take security threatening actions, primarily because the interface of a technology either keeps them from completing desired tasks or slows them down [16]. Interface design based on "error-avoiding principals" discourages human error that leaves systems vulnerable. If interface features can keep people from making mistakes, then privacy, through improved security, is better protected [17].

1.3 Privacy as Boundaries

Privacy is defined as any private or public space, real or virtual, that has an expected freedom from observation of action or personal information through monitoring. A bedroom is an example of a real space of expected freedom from monitoring and an email account is an example of a virtual space. Privacy as boundaries is similar to privacy as seclusion. However, seclusion generally applies to an individual. Privacy as boundaries differs in that it explicitly considers certain social settings and group activities [18]. It also treats concepts of time [19] and system memory [20] as bounded spaces that have attached privacy expectations. "It may be more profitable to think of privacy…in terms of the confluence of various boundaries, both physical and virtual" [21].

1.4 Privacy as Contextual

In this approach, the relevance of privacy issues is determined by the type of technology intended and the special characteristics of the users of the technology. It is less abstract and more easily conceived as a part of design decisions than other concepts [3]. Needs-analysis and attention to the user's relationships provide insight into user needs. This context-specific and user dependent approach to understanding privacy issues in design provides a more comprehensive definition of privacy. [22]. Given the variable nature of design processes, a contextual concept of privacy may have the most potential to provide designers with a definition that can inform design of technology and ensure a user-centered approach specifically when privacy is vulnerable.

2. The Context

A design relevant definition of privacy must be flexible and context aware. Subsequently, defining context becomes essential. Context is spatial and situational but only in relationship to a user. The user defines the context and the relevance of space and situation. In the case of designing technology for the elderly, it is essential to understand the attitudes and concerns related to privacy that are unique to this group. Seniors want to stay in their own homes as long as possible (23) and are willing to trade some amount of privacy for prolonged independence [24]. However, they want control over the type and amount of information shared and with whom it is shared. This control enhances their feeling of independence and creates trust of the technology [25, 26]. Most importantly, a feeling of control over personal privacy is essential to basic human dignity and elder well-being [27]. Accordingly, finding out which privacy concerns are most important to elders, who chose to continue to live at home while receiving living assistance, is essential to ensuring quality of life in later years.

Examining existing concepts of privacy, in terms of relevance to the types of technology that might be used in homes of elders [28], will provide insight into practical applications of privacy concepts in design. Some of these types of technologies are:

Sensing: detect movement, vibration, and vital statistics

Monitoring: Can use sensors or be interface dependant. Detect changes in daily activity or medical condition or progress in cognitive maintenance /enhancement activities

Communication: Telephones, monitors, handheld devices, alerting devices, ambient devices to maintain connection with family and community, life long learning and notification of caregivers.

Notably, a large part of the information that will be gathered in this environment will be health and medical information. Therefore, it is protected by HIPAA, the Health Insurance Portability and Protection Act (HIPAA) [15].

Information that falls under protection by HIPAA [29] includes:

> "The Privacy Rule protects all *'individually identifiable health information'* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.... is information, including demographic data, that relates to:
>
> • the individual's past, present or future physical or mental health or condition,
>
> • the provision of health care to the individual, or
>
> • the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual."

In general, this information cannot be shared with a third party without written patient consent. Also, if information is shared, the patient has the right to know. So the way that medical information in the home is handled must be considered differently than non-medical information.

3. Scenarios

In the following scenarios we will demonstrate privacy-aware design considerations that are informed by the concepts of privacy we discussed earlier in this paper.

> Gloria is a 75 year old mother of 3 and grandmother of 7. Her husband died 3 years ago and she now lives alone. One son lives in another state with his family but stays in touch with her by phone and email regularly. Her daughter lives in the same town but works a full-time job and has 4 children. She visits her mother 2 times a week. Her second son lives in the same town but rarely visits. He has a serious gambling habit and has alienated everyone except his mother. Gloria has minor health problems, mild arthritis and poor vision, but she is in overall good health. She is fiercely proud of her independence and quickly refused to move in with her son when her husband died. She wants to stay in her own home in the same town with her friends and younger grandchildren.
>
> To enable Gloria to stay at home with minimal intrusion, the family has decided to invest in home-based technology. Together with her physician, they decided to take a preventative and holistic approach to her independent living. They will use the smartest devices they can afford to make it easier for her to perform daily tasks, stay aware of her physical health, maintain her cognitive health, keep in touch with her family, lifelong friends, new Euchre club friends from the local community center, and medical care givers. Although Gloria mainly uses only her television, stereo system and land-line telephone for entertainment and communication, she is open to learning how to use new devices, especially if they will make her life easier. Given her activities and goals, what types of devices will do that? Given her experience with technology, what types of devices would she enjoy using? What types of interfaces would help her use the devices properly?

> Gloria uses health maintenance supplies on a daily basis. She is on a limited, fixed income and her family is struggling to help her financially. She already feels like she is taking money from them that could be used for her grandchildren. A friend recommends a discount online pharmacy that will give her a substantial discount if she provides personal shopping preference information. Sensors in her kitchen track meal times and food that she prepares and purchases regularly. Should non-medical data be available to the discount provider? If so, who should be able to grant permission, what level of detail should be available? How will her medical information be protected? Is there a guarantee that she will be aware of information shared with the provider? How clear are the terms of use of the provider? Should her children know about the discount agreement?
>
> Gloria is fine with her daughter knowing embarrassing details about her physical health but doesn't want her son-in-law or grandchildren to know that she has become incontinent. Although she doesn't have any serious medical conditions related to her incontinence, it may warn her physician and daughter of changes in her physical or emotional health. If they decide to collect this type of data, how will Gloria know that only her daughter and doctor will see this information? If she decides she doesn't want this information collected, does she the ability to say no?
>
> Gloria's house has been equipped with a monitoring system that identifies and tracks the people entering her house. Her gambling son visits her one day just to see how she is doing. Her daughter can retrieve information about who has been visiting her mom. When an expensive bracelet is missing, she confronts her brother. Gloria is upset by the accusation and ensuing argument and even more upset when she finds the bracelet that she had misplaced. She wishes she could have erased her sons visit from the record to avoid the stressful situation. Should Gloria be able to manage that information? If someone is taking advantage of her the information is valuable. However, Gloria wants to feel that she has control over whom she chooses to see and who knows about it.

In these scenarios, we try to show how these privacy issues could touch the lives of real people. we particularly want to stress the concept of privacy as contextual and context as personal in this example. Privacy issues are intrinsically tied to the personal attitudes of the individual and inextricable from quality of life and relationships in this home-based pervasive environment.

4. Privacy in Context

A contextual framework of privacy is particularly compatible with pervasive environments as pervasive technology design is also context aware and physical location alone cannot define context [30]. Restricting design context to physical location alone is too narrow because of the variability of user activities and the ever changing nature of information sharing and communication devices. Context can be extended to include actions, interactions and social activity [31]. So, like a contextual definition of privacy, this design approach to understanding context is flexible and changes as the technology and user changes.

Additionally, the intimate nature of pervasive technology in the home requires extreme attention to the needs and vulnerabilities of the user. Because user needs and contexts vary, a customizable framework for the design and evaluation of technology is needed.

For example, a privacy-aware, human-centered approach considers privacy issues in terms of the human user, as well as the need for a particular type of information about that user and the functionality of the device. Most importantly, context cannot exist in a space without the presence of a person Ultimately, the person creates context when they enter the space. A framework for privacy-aware design, with person-as-context, might be defined in the following way.

- ❖ People carry context with them into whatever space they occupy.

- ❖ Context is ever changing and influenced by immediate space, structures or sub-spaces, and objects in the space.

- ❖ The context is defined by the personal significance of purpose, message, and relationships of the space, structures and objects.

- ❖ Message is defined as the explicit and implicit expectations of the nature of space, structure or object.

- ❖ Privacy implications would be a characteristic of

    - o the message, purpose, and relationships of space, structure and objects

    - o the goals, needs, behaviors and relationships of the person.

    - o The interface of the objects

- ❖ Remote space is also a component of context but has different characteristics than immediate space.

These are some design considerations that might apply:

Consider Message:

- What does the space communicate about privacy?
- Is this message misleading?
- Is monitoring implicit or explicit?
- How transparent is the technology?

Consider Purpose:

- To what degree does the intended use threaten privacy?
- Can misuse or unexpected use threaten privacy?

Consider Relationships:

- Who will have access to the remote space, immediate space, structures, and objects of the user?
- How many and what types of people will have permission to access user data?
- What types of data should, by default, be restricted to the user?
- What is the relationship between different objects in the environment?
- What are the relationships with objects and people in other spaces?

Consider Interface:

- Does the interface afford control of privacy preferences?
- Is the interface misleading about level of privacy protection provided?
- What level of abstraction or interpretation of privacy functionality is necessary?
- How can visualization of sensitive data preserve privacy?
- How can the interface increase user awareness of possible privacy threats?

Consider Goals

- How will user experience goals affect the integrity of privacy design features?
- How are the personal life goals of the person affected by privacy issues?

Consider Behaviors

- What types of recreational or social activity of the person might be privacy threatening?
- Does the person have an attitude that is compatible with risk awareness? For example, are they more likely to trust something new or be suspicious of it?

Consider Needs

- How much does the user want to know about how the technology works?
- What are the privacy concerns of the user?
- How much visibility of privacy related functionality is appropriate for the user?
- Could the design allow for changing privacy needs?
- Is level of privacy in line with user expectations?

This design framework treats privacy as an element of context so it requires the designer to think about privacy at every stage of the design process. For this reason, the designer actively considers the vulnerabilities of the user. The focus on the context of the user, in this case an elder in a home environment, requires the designer to embed the privacy related goals, needs and behaviors of the user into the designs.

From these considerations, the designer will be able to draft a set of context specific questions within this framework. Asking these questions allows the designer to embed the user's preferences into the conceptual phase of the design process. Before any technologies are introduced into a home, user needs determine which objects or structures in the house should even be considered for implementation in the pervasive environment.

This approach to design provides a structure for thinking about the privacy implications of home based pervasive technology that is user-focused, practical and flexible. This framework also allows for an evolving definition of privacy; as technology changes, privacy implications change.

5. Questions of Context

After asking general information questions about home, rooms (structures) in the home, frequently used objects in the home, daily home activities, and personal relationships, the designer can then ask questions directly related to privacy concerns of the user.

Privacy attitudes about home

1. When you are at home, who should be able to know about how you are doing?
2. What types of things should they be able to know?
3. Do you want to always know when someone learns something about you?
4. Would you always want to be asked for permission?

Privacy attitudes about spaces in the home

5. Would you feel comfortable leaving a visitor or guest in your home alone in (room a-h) when you were in another room?
    a. Living room
    b. Kitchen
    c. Dining room
    d. Bedroom
    e. Bathroom
    f. Foyer
    g. Basement
    h. Garage

Privacy attitudes about objects

6. Describe some of your favorite things [object1-objectX] in your home to me?
7. Do you ever share [object1-objectX] with someone else?
8. Would you ever want to share [object1-objectX] with someone else?
9. If [object1-objectX] could learn things about your health would that be okay with you?
10. What types of things should it be able to know?
11. Do you want to always know when this object learns something about you?
12. Would you always want to be asked for permission?
13. If [object1-objectX] could learn things about your daily activities would that be okay with you?
14. What types of things should this object be able to know?
15. Do you want to always know when it learns something about you?
16. Would you always want to be asked for permission?
17. If [object1-objectX] could learn things about your social life would that be okay with you?
18. What types of things should it be able to know?
19. Do you want to always know when it learns something about you?
20. Would you always want to be asked for permission?

21. If [object1-objectX] could learn things about how often you communicate with family and friends would that be okay with you?
22. What types of things should it be able to know?
23. Do you want to always know when it learns something about you?
24. Would you always want to be asked for permission?

This list is not exhaustive; it represents the types of questions that could be asked based on this framework.

6. Conclusion and Future Work

Although many definitions of privacy exist, defining privacy in terms of context is a practical and useful approach to privacy-aware design of pervasive home-based technologies for elders. More information about the specific attitudes of elders related to privacy and technology will allow designers to better address elders' privacy related needs in this environment. To gain more insight into the privacy concerns of this particular user group, we will be conducting ethnographic observations and interviews of elders in their homes. The interviews will consist of questions derived from the contextual framework. This dialogue with the target group will uncover more specific privacy-focused design considerations for this environment.

In conclusion, privacy-awareness in technology design is essential for any designer and especially when designing for intimate pervasive spaces. As new technologies emerge, the privacy impact of those technologies is ultimately determined by the relationship between the design, the user, and public policy. Although the design alone can not guarantee privacy preservation, continued research that involves active feedback from the user will enhance understanding and awareness of privacy implications of technology and will enable privacy-preserving rather than privacy-threatening designs.

References

[1] Tufte, E. R. Envisioning information, Graphics Press, Cheshire, CT, 1990

[2] Reidenberg, J ''Privacy wrongs in search of remedies,'' *Hastings Law Journal*, 54, 877–898, 2003.

[3] Boyle, M. "A Shared Vocabulary for Privacy," presented at Fifth International Conference on Ubiquitous Computing, Seattle, Washington, 2003.

[4] Shostack, A. and Syverson, P. "What Price Privacy?" in Camp, L. Jean and Lewis, Stephen (editors.) *Economics of Information Security* (2004) Springer/Kluwer

[5] Huberman, B.A., Adar, E., Fine, L.R.: Valuating Privacy. Fourth Workshop on the Economics of Information Security (WEIS05), Cambridge, MA (2005), http://infosecon.net/workshop/pdf/58.pdf

[6] Friedman, B., Hurley, D., Howe, D. C., Nissenbaum, H., and Felten, E. 2002. Users' conceptions of risks and harms on the web: a comparative study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems* (Minneapolis, Minnesota, USA, April 20 - 25, 2002). CHI '02. ACM, New York, NY, 614-615.

[7] Camp, L. J., Osorio, C. A., "Privacy-Enhancing Technologies for Internet commerce," in *Trust in the Network Economy*, O. Petrovic, M. Fallenbock, and C. F. Kittle, Eds. Springer, January 2003.

[8] Bellotti, V. and Sellen, A. "Design for Privacy in Ubiquitous Computing Environments", Proc. Third European Conference on Computer-Supported Cooperative Work ECSCW'93, Milano, Italy, September 13-17, 1993.

[9] Bartow A Feeling of Unease About Privacy Law. *University of Pennsylvania law review* vol:154, 2006.

[10] Warren &Brandeis "The Right to Privacy" *Harvard Law Rev.,* vol. 4, no. 5, Dec.1890, pp. 193–200.

[11] Camp "Designing for Trust" in Trust, Reputation, and Security: Theories and Practice. R. Falcone, Ed., Springer-Verlag, 2003.

[12] Lessig, L. Code and Other Laws of Cyberspace, Basic Books, Inc., New York, NY, 1999.

[13] Hochheiser, H. 2002. The platform for privacy preference as a social protocol: An examination within the U.S. policy context. *ACM Trans. Inter. Tech.* 2, 4 (Nov. 2002), 276-306.

[14] Vila, T., R. Greenstadt, and D. Molnar. 2004. Why we can't be bothered to read privacy policies: Models of privacy economics as a lemons market. In Economics of Information Security. Vol 12 of Advances in Information Security, eds. L.J. Camp and S. Lewis, 143--154. Boston: Kluwer Academic Publishers.

[15] Swire, P. and Steinfeld, L. 2002. Security and privacy after September 11: the health care example. In *Proceedings of the 12th Annual Conference on Computers, Freedom and Privacy* (San Francisco, California, April 16 - 19, 2002). CFP '02. ACM, New York, NY, 1-13.

[16] Dourish, P. and Redmiles, D. 2002. An approach to usable security based on event monitoring and visualization. In *Proceedings of the 2002 Workshop on New Security Paradigms* (Virginia Beach, Virginia, September 23 - 26, 2002). NSPW '02. ACM, New York, NY, 75-81.

[17] Maxion, R., Reeder, R. Improving user-interface dependability through mitigation of human error. *International Journal of Human-Computer Studies* Volume 63, Issues 1-2, July 2005, Pages 25-50

[18] Jiang, X. Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social; Jiang, X. Ubicomp 2002 Workshop on Socially Informed Design of Privacy- Enhancing Solutions in Ubiquitous Computing); 2002, Göteborg, Sweden.

[19] Langheinrich, M. Privacy Invasions in Ubiquitous Computing. 'Privacy invasions in ubiquitous computing', paper presented at Ubicomp 2002 Privacy Workshop, Göteborg, Sweden, [online] Available at http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/uc2002-pws.pdf

[20] Stajano, F. "The Resurrecting Duckling – What next?" in Security Protocols—8th International Workshop, Lecture Notes in Computer Science, Cambridge, United Kingdom, Apr. 2001. Springer-Verlag, Berlin Germany.

[21] Shapiro, S., `Places and Spaces: the Historical Interaction of Technology, Home, and Privacy', The Information Society14: 275-284. 1998

[22] Camp, L.J., Connelly, K., Shankar, K., Design for Privacy: Towards a Methodological Approach to Trustworthy Ubicomp Design., in Proceedings of ETHICOMP 2005 (Linköping, Sweden) 12 -14 September, 2005.

[23] A.-H. Bayer and L. Harper, *Fixing to Stay:A National Survey on Housing and Home Modification Issues—Executive Summary*, Am. Assoc. Retired Persons, 2000;
http:// research.aarp.org/il/home_mod_1.html

[24] Applebaum, R., Straker, J. Long-Term Care Challenges for an Aging America: Improving Technology and Changing the System's Culture as Critical Parts of the Solution *Public Policy & Aging Report* Volume 15, Number 4, 2005.

[25] Consolvo, S., Roessler, P., Shelton, B., The CareNet Display: Lessons Learned from an In Home Evaluation of an Ambient Display. Proceedings of the 6th Int'l Conference on Ubiquitous Computing: UbiComp '04, (Sep 2004), pp.1--17.

[26] Fox, S. `Trust and Privacy Online: Why Americans Want to Rewrite the Rules', Pew Internet & American Life Project, August, 2000. URL accessed on 12/10/07.: http://www.pewinternet.org

[27] Jacelon C. S. The dignity of elders in an acute care hospital. *Qualitative Health Research*; 13: 543–556. 2003

[28] Mynatt, E. D., Rowan, J., Craighill, S., and Jacobs, A.Digital family portraits: supporting peace of mind for extended family members. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Seattle, Washington, United States). CHI '01. ACM, New York, NY, 333-340, 2001.

HIPPA information from http://www.hhs.gov/ocr/privacysummary.pdf URL accessed on 12/15/07.

[29] United States Department for Health and Human Services "Summary of the HIPAA Privacy Rule" available at http://www.hhs.gov/ocr/privacysummary.pdf accessed on 10/15/07.

[30] Dourish, P., Grinter, R. E., Delgado de la Flor, J., & Joseph, M. Security in the wild: User strategies for managing security as an everyday, practical problem. Pers Ubiquit Comput, 8, 391–401, 2004.

[31] Dourish, P, What we talk about when we talk about context. *Personal and Ubiquitous Computing*, 8(1), 19–30. 2004

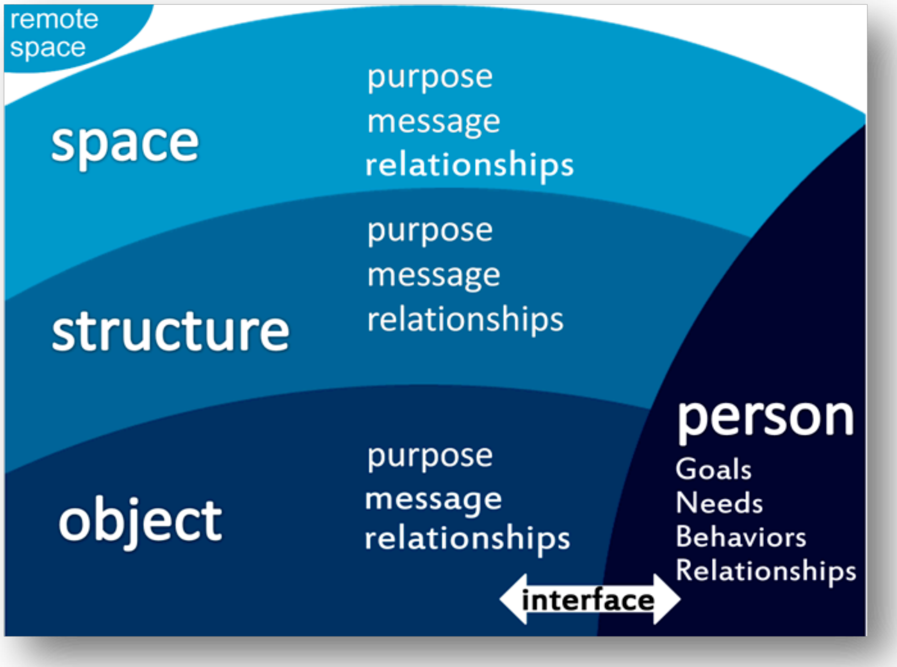

Figure 2 Person-as-Context Framework diagram

This material is based upon work supported by the National Science Foundation under award number 0705676. Any opinions, findings, and conclusions or recommendations expressed in this presentation are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.