A Shared Vocabulary for Privacy

Michael Boyle

University of Calgary
boylem@cpsc.ucalgary.ca

Irwin Altman's popular theory of privacy as a normalizing, dynamic, dialectic process regulating self-environment interactions is integrated with observations and conceptions of privacy drawn from ubicomp, law, architecture, sociology, and psychology. The result is a unified, holistic and comprehensive vocabulary for discussing privacy issues in the design of ubicomp systems, specifically ubiquitous video media spaces. The full vocabulary is rich with subtleties, and this paper presents a summary of material presented elsewhere [7]. The key elaboration of Altman's theory deconstructs privacy into three synergistically-coupled genres of *control* of self-environment boundaries. *Solitude* controls interpersonal interactions and *attention*. *Confidentiality* controls information access and *fidelity*. *Autonomy* controls observable manifestations of *identity*.

Motivating a shared vocabulary for privacy

My research on privacy began with the goal of designing and building reactive ubiquitous video media space (VMS) environments that use video obfuscation techniques to balance privacy concerns against awareness needs for intimate collaborators. Like most other ubiquitous computing applications, video media spaces are an interesting crucible for the study of privacy in the design of CSCW tools because a broad spectrum of (hard) design challenges have emerged from numerous researchers' practical experiences designing, building, and ultimately living with always-on video. My particular work bridged off from Greenberg and Kuzuoka's Active Hydras and physically-based digital surrogates for informal awareness and casual interaction [14]: I conducted a controlled experiment to narrow in on the applicability of video pixelization and blurring distortion filtration to resolving privacy-awareness tensions [6].

My progress came to a halt because I did not have sufficient understanding of what privacy is in order to competently and appropriately design user interactions that support its preservation. While a significant amount of privacy-related theory and practice concerning the design of video media spaces has come out of the HCI research community, privacy is an overwhelmingly large and nebulous concept—even after reviewing this literature I found myself lost when trying to attack the privacy-preserving VMS design problem using a bottom-up design-build-test methodology. In some cases, I was made even more confused after surveying existing literature: various researchers use common words differently (e.g., using privacy to refer to both freedom from distraction [16] and keeping secrets [1]) or use different words to refer to the same phenomenon (e.g., using solitude [25] to mean isolation [2]).

Cite as:
Boyle, M. (2003) A Shared Vocabulary for Privacy. In *Workshop on Ubicomp Communities: Privacy as Boundary Negotiation.* Held as part of the UBICOMP'2003 5th International Conference on Ubiquitous Computing, Seattle, October 12.

I felt I lacked the vocabulary needed to articulate design problems and the consequences of design choices. Thus I began a long exploration of privacy, drawing upon the theoretical and philosophical thinking and empirical observations found in such disciplines as behavioral psychology, sociology, architecture, law, and anthropology. Along the way, I assembled a broadly and deeply articulated vocabulary for discussing privacy-related concepts as they apply to video media space design. In this paper I wish to summarize this "lexicon for privacy" [7] by elaborating on a number of key integrations and extensions we have made to others' discussions of privacy.

Foundation for deconstructing privacy

Like other researchers in computers and privacy (e.g., Palen and Dourish [22]) I begin with Irwin Altman's broadly articulated theory of privacy regulation, emphasizing a *self-environment boundary regulation process* based on *dynamic*, *social*, *dialectic normalization of desired* privacy to *attained* levels [2,3]. Altman's theory of privacy as a process involving a rich palette of individual and social human behaviors—e.g., personal space and territory—has great "heuristic appeal" [8] for researchers, yet it is frustrating to use his theory directly. While it is broad enough (somewhat necessarily) to be used to analyze any privacy-design problem in ubicomp, it is articulated at such an *abstract* level that it is hard to apply it directly to concrete design challenges. Moreover, Altman generated his ideas long before people had much experience living with ubicomp technologies. Without 'concrete links' it is difficult to reconcile Altman's ideas with recent technological developments and experiences.

The over-arching elaboration Altman's theory I make incorporates Ruth Gavison's decomposition of privacy into three basic elements [13]:

- *Solitude*: control over one's interpersonal interactions with other people.
- *Confidentiality*: control over other people's access to information about oneself.
- *Autonomy*: control over what one does, i.e., freedom of will.

Gavison also emphasizes the role of *control* in privacy management, and that genuine control requires both an abundance of options to choose from and the power to ensure that one's choice is respected by others. Gavison's discussion yields powerful vocabulary which I will use to disambiguate the many interrelated meanings of privacy discussed by Altman. By discussing privacy in terms of controls, I am deconstructing the mechanical aspects of self-environment boundary regulation, side-stepping the much more difficult deconstruction of the boundary itself taken up by Palen and Dourish [22]. The two approaches are, however, very complementary, and direct parallels between them will be discussed throughout this paper.

I claim here that Altman's normative dialectic process regulates the self-environment boundary by way of these three genres of control, where individual and social human behaviors (such as those discussed by Altman and Chemers [3] and Langheinrich [18]) are the low-level mechanical means by which control is exerted. I assume Dennet's model of control [11]. Therefore, from the perspective of a single individual, all three genres of control are exercised concurrently: behaviors used to exert one kind of control also have strengthening and weakening implications for the

other kinds of control. Hence, *choice* is important: it is only with an abundance of ways to conduct interpersonal interactions, access information, or behave that people might be able to successfully regulate the porous, membrane-like self-environment boundaries that Altman describes. Taking this one step further, we see that to have genuine control over solitude, one must have opportunities to be *with* others as well as apart from them. Similarly, to have genuine control over confidentiality, one must have opportunities to disclose information to others as well as conceal it.

Furthermore, the privacy-related actions of one individual operate concurrently with those of all other individuals: Altman's notion of attained privacy is thus the net effect of all these mutually, complementary, and competitively interacting privacy-affecting actions. Gavison's remarks about privacy as a social power and Dourish's discussion of cultural factors affecting technology design [12] relate here: although some people may have more privacy options and more power in certain dominions, rarely does any one individual have control over all facets of his privacy to the exclusion of all others. This observation prompts reconsideration of the competitive (i.e., greedy) sort of privacy necessarily emphasized in law and computer security-related disciplines. Trust permits people opportunities to enjoy the rewards of interacting with others even though these interactions may put their privacy at risk. This risk-reward tradeoff is important to ubicomp design. Risks typically accrue with reward, yet there are many examples in prior work in video media spaces in which the design of the media space confounds this risk-reward relationship, e.g., as in the case of family members in a media space connecting telecommuters at home to office colleagues [20].

Although this deconstruction of privacy into solitude, confidentiality and autonomy controls serves to disambiguate some of the varied connotations of the word privacy, it is still woefully incomplete. There are aspects of privacy discussed in the CSCW literature which do not fit e.g., Hudson and Smith's discussion of distraction and salience [16], or Zhao and Stasko's work on various video filtering techniques [26]. In the following sections, I make a few small, but important, scope-widening enhancements to the meanings of solitude, confidentiality, and autonomy that permit incorporation of what we in CSCW have learned about the effects of technology and user interface design on privacy regulation.

Extending solitude by incorporating attention

Westin [25] decomposes privacy into four states: solitude (i.e., isolation), intimacy; anonymity (i.e., going unnoticed in a crowd); and, reserve (i.e., using psychological barriers to ignore others near-by). Although Westin's isolation and intimacy states easily fit in with our notion of solitude—they become like two points on a broad spectrum of interpersonal distances—anonymity and reserve seem quite different. Both refer to the idea of being noticed, i.e., *attention*. *Consequently, I extend the scope of solitude to include control over attention*.

For this discussion, I assume a model of capacity constrained focal working memory and a selectively filtering peripheral working memory that prioritizes collected stimuli according to heuristics like "enduring dispositions" and "momentary intentions." This model is derived from Reason [23] and Norman [21], and highlights mechanical ways people control attention by regulating which stimuli are sensed from

the environment e.g., personal space [15] and reconfiguring architectural permeability to light, matter, and sound. Gavison's point that attention is a primary means of information gathering [13] illustrates the strong relationship between solitude and confidentiality. Moreover, by placing the regulation of attention as a component of privacy regulation, a coherent picture emerges of how ubicomp issues like distraction and camera shyness [19] relate to privacy.

Extending confidentiality by incorporating fidelity

Here, *fidelity* is taken to be a subjective, perceived understanding of the accuracy (e.g., correctness) and precision (e.g., detail) of the capture, representation or presentation of information. The same essential truth can be expressed at a variety of fidelities: vague descriptions may be accurate but imprecise; misinformation is neither accurate nor precise; disinformation can be invented to be precise and yet be quite inaccurate; and so forth, along both axes of the fidelity space. There is a distinction between fidelity and sensitivity [1], yet the two are related: the severity of harmful outcomes arising from others' (undesired) access of sensitive information increases with the fidelity at which it is accessed. *I extend the scope of confidentiality to include control over the fidelity at which information is accessed by others.*

This extension unifies many mechanisms for preserving privacy: content control techniques such as video obfuscation [6,26], traditional access control and cryptographic techniques [24], territoriality and personal space. It also complements Palen and Dourish's discussion of information disclosure self-environment boundaries [22] and prompts reconsideration of the tension between privacy and informal awareness. The two have been typically presented in opposition to each other: in order for one person to have more privacy, others must necessarily have less awareness of him [16]. However, Palen and Dourish point out instances in which the judicious revalation of informal awareness cues is vital to ensuring that one has the solitude or autonomy one desires [22].

Although one must necessarily keep the concepts of *access* and *information* free from the limitations of a constraining definition, one can nonetheless consider that some accesses have the potential to *change* the perceived fidelity of some information. A few examples will explain. Broadcasting misinformation to a wide audience does not magically change its true accuracy but it can certainly increase its *perceived* accuracy. Small bits of information may be shared among third parties so that each has a much higher fidelity view of the whole. Information may be processed so as to change the fidelity of other information e.g., generating good predictions of the future, making inferences of the past, correlating information, making abstractions and generalizations to better comprehend complex phenomena, or convincingly fabricating false information. Lastly, similar to Palen and Dourish's discussion of temporal boundaries, we can consider that while the fidelity of human memory decays with time, technology capable of storing information changes this rate of decay—turning the ephemeral into the perpetual—and thus confounds regulation of confidentiality. Taken together, these examples help motivate Westin's assertion that the right to privacy includes some degree of control over information about the self that others collect and transmit and the right to verify the accuracy of the information.

Extending autonomy by incorporating identity

Autonomy, as has been presented thus far, is the freedom to do as one wants without interference from others. Yet, the conception as a whole is awkward to work with because it is not presented as a genre of control. Indeed, freedom is much like a control in that it involves choice of action, i.e. behavior, and the power to ensure that others do not coerce or constrain the behavior. This control-over-behavior conception of autonomy, however, does not account for Bellotti's observation that video media spaces fail to present sufficient and appropriate contextual cues to support self-appropriation [4]. Bellotti further notes that the subsequent dissociation and disembodiment problems inherent in the media space not only prompt opportunities for inadvertent privacy violations but also heighten user and non-user apprehension towards the technology. Control-over-behavior also does not account for the weight that Altman himself places on *self-definition* as a function of privacy.

The concept that unifies behavior, appearance, impression, and self-definition is *identity*. Here, identity is a complex thing comprised not only of external projections like behavior, appearance and impression but also the internalizations that drive them, such as temperament and attitudes, personal experiences in life, name, gender, nationality, and so forth. *Consequently, I extend the scope of autonomy to include control over the definition and observable manifestation of one's identity.*

Autonomy is a constrained control because I have placed it within Altman's framework of a dialectic privacy process. Genuine control over autonomy includes times when one relents to the will of others and chooses not to get his/her own way. For instance, in law one's freedoms are constrained by the rights of others. Bellotti's discussion of self-appropriation behaviors [4] illustrates how expectations of behavior (e..g., culture and role relationships) are in fact mutually held mechanisms for regulating autonomy. Moreover, her discussion of contextual cues for self-appropriation underscores Altman's claim that privacy is a dynamic (i.e., situated) process and relates to Neustaedter's [20] discussion of how the lack of architectural transitions between home and office cultures in a media space results in autonomy problems like role conflict.

Lastly, since information about a person's identity (e.g., his actions, his utterances) can be recorded in computer files, personal documents, and other artifacts physically separable from one's body or mind, incorporating identity into the scope of autonomy underscores synergisms with confidentiality and introduces into the discussion whole classes of ubicomp technologies [10] devoted to controlling access to personally identifying information e.g., anonymizers.

Summary

I have assembled a shared vocabulary for privacy that reconciles Altman's theory of dialectic privacy with the varied observations and deliberations of many other privacy researchers. The vocabulary was necessary when it became clear to me that I lacked a sufficiently broad and deep understanding of privacy to continue my bottom-up methodology for designing and building a privacy preserving video media space. Only the essential aspects of this lexicon for privacy have been mentioned here; a myriad of subtleties have been abbreviated. Although the work of Irwin Altman

served as a crucial seminal starting point, it was important to weave into his discussion the vocabulary and conceptions of privacy developed in other disciplines—especially ubicomp and other design-related disciplines like law and architecture—so that Altman's abstract theory could be applied to the concrete design problems ubicomp researchers face.

The vocabulary I described here deconstructs Altman's normative, dynamic, dialect self-environment boundary regulation process into a triad of solitude, autonomy, and confidentiality controls. I broadened the scope of solitude to include control over attention, and in doing so found ways to incorporate into the theory ubicomp design issues like distraction and camera-shyness. I broadened the scope of confidentiality to include control over fidelity of information accessed, and in doing so found ways to incorporate a rich palette of work in the CSCW community on content control in media spaces. Finally, I broadened the scope of autonomy to include control over the observable manifestations of identity, and in doing so found ways to incorporate rich social theory on self-appropriation, role conflict, and work done in the CSCW and computer security communities. This broadly articulated theoretical groundwork has already been put to use, helping to drive the design and analysis of Neustaedter's context aware home media space [20].

Acknowledgements

I would like to thank Gregor McEwan at the University of Calgary for his advice and assistance producing this paper.

References

1. Adams, A. 2000. Multimedia Information Changes the Whole Privacy Ballgame. In *Proceedings of Computers, Freedom, and Privacy* (CFP 2000, Toronto), ACM Press, New York, NY, 25–32.
2. Altman, I. 1975. *The Environment and Social Behavior*. Brooks/Cole Publishing, Monteray, CA.
3. Altman, I., and Chemers, M. 1980. *Culture and Environment*. Wadsworth Publishing Company, Stamford, CT.
4. Bellotti, V. 1998. Design for Privacy in Multimedia Computing and Communication Environments. In Technology *and Privacy: The New Landscape*, P. Agre and M. Rottenberg, Eds. MIT Press, Cambridge, MA, 63-98.
5. Bellotti, V., and Sellen, A. 1993. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work* (ECSCW'93, Milan), Kluwer Academic Publishers, Dordrecht, 77-92.
6. Boyle, M., Edwards, C. and Greenberg, S. 2000. The Effects of Filtered Video on Awareness and Privacy. In *Proceedings of the Conference on Computer Supported Cooperative Work* (CSCW'2000, Philadelphia), ACM Press, New York, NY, 1–10.
7. Boyle, M. and Greenberg, S. 2003. *A Lexicon for Privacy in Video Media Spaces*. Report 2003-724-27, Department of Computer Science, University of Calgary.
8. Brierley-Newell, P. 1995. Perspectives on privacy. In *Journal of Environmental Psychology*, 15, Academic Press, New York, NY, 87–104.

9. Brierley-Newell, P. 1998. A cross-cultural comparison of privacy definitions and functions: A systems approach. In *Journal of Environmental Psychology*, 18, Academic Press, New York, NY, 357–371.
10. Burkert, H. 1998. Privacy-Enhancing Technologies: Typology, Critique, Vision. In *Technology and Privacy: The New Landscape*, P. Agre and M. Rottenberg, Eds. MIT Press, Cambridge, MA, 125-142.
11. Dennet, D. 1995. *Elbow Room: The varieties of free will worth wanting*. MIT Press, Cambridge, MA.
12. Dourish, P. 1993. Culture and Control in a Media Space. In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work* (ECSCW'93, Milan), Kluwer Academic Publishers, Dordrecht, 125–138.
13. Gavison, R. 1984, Privacy and the limits of law. In F. Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, New York, NY.
14. Greenberg S., and Kuzuoka, H. 2000. Using Digital but Physical Surrogates to Mediate Awareness, Communication and Privacy in Media Spaces. *Personal Technologies*, 4:1 (January). Elsevier.
15. Hall, E.T. 1966. *Distances in Man: The Hidden Dimension*. Double Day, Garden City, NY.
16. Hudson, S.E., and Smith, I. 1996. Techniques for Addressing Fudamental Privacy and Disruption Tradeoffs in Awareness Support Systems. In *Proceedings of the Conference on Computer Supported Cooperative Work* (CSCW'96, Cambridge), ACM Press, New York, NY, 248-247.
17. Kelvin, P. 1973. A Social Psychological Examination of Privacy. In *British Journal of Social and Clinical Psychology*, 12, Swets & Zeitlinger, Lisse, 284-251.
18. Langheinrich, M. 2001. Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems. In *Proceedings of UbiComp 2001* (Atlanta), Springer, New York, NY, 273-297.
19. Lee, A., Girgensohn, A., and Schlueter, K. 1997. NYNEX Portholes: Initial user reactions and redesign implications. In *Proceedings of the ACM/SIGGROUP Conference on Groupware* (GROUP'97, Phoenix), ACM Press, New York, NY, 385–394.
20. Neustaedter, C. and Greenberg, S. 2003. The Design of a Context-Aware Home Media Space. To appear in *Proceedings of UbiComp 2003 Fifth International Conference on Ubiquitous Computing*.
21. Norman, D. 1976. Memory and Attention (2nd Edition). John Wiley & Sons, Inc. Toronto, ON.
22. Palen, L., and Dourish, P. 2003. Unpacking Privacy for a Networked World. In *Proceedings of the Conference on Human Factors in Computing Systems* (CHI 2003, Ft. Lauderdale), ACM Press, New York, NY, 129-137.
23. Reason, J. 1990. *Human Error*. Cambridge University Press, New York, NY.
24. Smith, I.E., Scott, E.H., Mynatt, E.D., and Selbie, J.R. 1995. Applying Cryptographic Techniques To Problems In Media Space Security. In *Proceedings of the Conference On Organizational Computing Systems* (COOCS'95, Milpitas), ACM Press, New York, NY, 190-196.
25. Westin, A. 1967. *Privacy and Freedom*. Atheneum, New York, NY.
26. Zhao, Q.A., and Stasko, J.T. 1998. Evaluating Image Filtering Based Techniques in Media Space Applications. In *Proceedings of the Conference on Computer Supported Cooperative Work* (CSCW'98, Seattle), ACM Press, New York, NY, 11–18.