# 1

# Privacy Issues and Human-Computer Interaction

**Mark S. Ackerman**

University of Michigan

**Scott D. Mainwaring**

Intel Research

Privacy can be a key aspect of the user experience with computers, online systems, and new technologies. Knowing what to consider about users and their views of computer systems can only improve privacy mechanisms. Human-Computer Interaction (HCI) is the subfield of Computer Science that studies how people interact with and through computational technologies. This chapter examines what HCI, as a research area, offers to both those designing and those researching privacy mechanisms.

HCI is a large research field in its own right. HCI's roots were in human factors and the design and evaluation of "man-machine" interfaces for airplanes and other complex and potentially dangerous mechanical systems. The first papers in what would later be known as HCI were in the 1970s and concerned the design of user interfaces in time-sharing systems. The field took off with the advent of personal computers and the single-user interface in the early 1980s. HCI's roots then were in cognitive-oriented, single-user interfaces – the so-called user interface.

HCI has since expanded to consider a variety of subareas – design methodologies, usability and usability testing, intelligent interfaces, adaptive interfaces, and so on. Of particular interest here will be Computer-Supported Cooperative Work (CSCW), sometimes known as groupware. CSCW is interested in how groups of people work or

interact together using computational technologies. Indeed, HCI has grown in general to consider organizational, institutional, and even societal factors affect how computer systems are put together and how users interact with systems.[1] This has become increasingly important as systems are no longer single-user, but are also Internet-wide in their use.

This chapter will largely view HCI in its broader context. HCI is not just about user interfaces but also about the *user experience* of systems: how people perceive and understand, reason and learn about, and react and adapt to digital technologies. To borrow the terminology Sasse and Flechais[2] use in discussing security, HCI has come to deal not only with *process* (how systems are used, designed, and developed) and *product* (the systems themselves and their interfaces), but also *panorama* (cultural and organizational contexts that support, discourage, or otherwise shape the systems they envelope). Privacy, like security, implicates all of these levels. It is by its nature both a question of the user and his or her data but also the user and others' use of that data. Our interests, therefore, will be those of HCI-writ-large.

While HCI has gone through several generations of computational technologies, it has carried a number of research themes forward. As mentioned, this chapter will consider the various HCI themes and their research findings that may be important when designing, constructing, or evaluating privacy mechanisms. Before exploring these HCI research streams, however, we first need a working definition of privacy, and to compare and contrast privacy concerns with HCI concerns.

# Privacy and HCI

This chapter necessarily juggles two somewhat amorphous terms, "privacy" and "HCI". HCI has already been introduced, along with its core concerns of improving ease of use and the overall user experience. Privacy, on the other hand, is an even broader term. Unlike "HCI," it's a term in everyday language, and so its meanings are rooted in larger cultural practices and understandings. It has technical meanings in, for example, law, ethics, and social theory, but also engenders strong, emotional connotations in common usage and daily experience.

For the purposes of this chapter, a simple but useful definition of privacy is "the ability of an individual to control the terms under which their personal information is acquired and used."[3] As such, privacy is about individuals' capabilities in a particular social situation

---

[1]Grudin, Jonathan. 1996. The organizational contexts of development and use. *ACM Computing Surveys*, 28 (1) : 169-171.

Grudin, Jonathan. 1994. Computer-supported cooperative work: History and focus. IEEE Computer, 27 (5) : 19-26.

[2]Sasse, M. Angela, and Ivan Flechais. 2005. The Case for Usable Security. In L. Cranor and S. L. Garfinkel (eds), *Designing Secure Systems That People Can Use*, O'Reilly & Associates, Cambridge,

[3]Culnan, Mary J. 2000. Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy and Marketing*, 19 (1) : 20-26.

to control what they consider to be personal data. Although fairly simple, this definition immediately raises a number of important points:

- Privacy is based on information and the effectiveness of individuals in controlling its flow, and so has a natural relationship with the concerns of HCI (as well as the field of computer security). Indeed, as systems have increasingly involved the processing of personal information, particularly in the context of financial and governmental transactions, issues of privacy have naturally risen in prominence within the field of HCI.
- Privacy, like security, concerns risk, its perception, and its management. Privacy problems often lie in the potential future consequences of present behavior, which may be deemed risky or safe according to standards of judgment (not necessarily those of the participants involved). As such, privacy harkens back to HCI's origins in ergonomics and the safe operation of complex machinery.
- Privacy is about control, trust, and power in social situations and so rapidly implies ethical, political, and legal issues. It appeals to notions of individual autonomy and freedom: control of one's person, and access to one's person, in the form of personal information.[4] But this freedom is almost always constrained and often may have to be traded off in certain transactions, such as to access credit or to maintain the quality of health care.[5] These are in general issues for social, behavioral, and political science, but HCI does include many useful examples of interdisciplinary applied research.[6].

As this chapter will argue, privacy is individually subjective and socially situated. Indeed, privacy, as part of social interaction in general, is not a unified experience. What may be privacy in e-commerce or online banking may be a very different problem for people than in social computing. Shortly below, we will see that people differ widely in their attitudes as well. That is, people's experience of privacy, their expectations and goals, and their problems concerning privacy may all differ when moving among areas of computation, society, and even tasks. We'll leave further discussion of the definitional problems inherent in "privacy" to other authors in this book, and use Culnan's broad definition. As we have seen, it suggests *prima facie* similarities between the concerns of HCI and of privacy at a number of different levels. It raises important issues as well, particularly regarding the irreducibility of privacy concerns to purely functional issues of efficiency and ease of use. The broader conceptions of HCI will be needed to deal with complex real-world social and ethical issues like privacy

---

[4]Altman, Irving. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*. Monterey, CA: Brooks/Cole Publishing.

[5]Clarke, Roger. 1999. Introduction to Dataveillance and Information Privacy, and Definition of Terms. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

[6]For example, see Friedman, Batya, Peyina Lin, and Jessica K. Miller. 2005. Informed Consent by Design. In L. Cranor and S. L. Garfinkel (eds), *Designing Secure Systems That People Can Use*, O'Reilly & Associates, Cambridge.

Goecks, Jeremy, and Elizabeth D. Mynatt. 2005. Social Approaches to End-User Security and Privacy Management. In L. Cranor and S. L. Garfinkel (eds), *Designing Secure Systems That People Can Use*, O'Reilly & Associates, Cambridge, .

We now turn to the relevant HCI research.

# Relevant HCI Research Streams

HCI, as is any scientific area, is composed of numerous research streams. We cannot hope to cover the field here. Useful surveys include the *Handbook of Human-Computer Interaction*[7] and *Readings in Human-Computer Interaction: Toward the Year 2000*[8], especially the chapter introductions). See also the annotated bibliography of HCI resources provided by Karat, Brodie, and Karat.[9]

In any case, several research streams within HCI are of immediate interest to the examination of privacy and the design of privacy mechanisms. These include:

- Basic design considerations – designing for general usability and the evaluating of usability (usability engineering).
- How people interact with and through systems (Computer-Supported Cooperative Work).
- How individuals differ in their capabilities and how that affects the human-computer interface (individual differences and tailorability).
- The role of HCI in next-generation architectures (ubiquitous computing, pervasive computing).

Each will be covered in turn.

## Usability Engineering

Over the last twenty years considerable interest and effort has gone into improving the usability of computers. Advances in the 1980s such as mice and GUI interfaces greatly expanded the market by removing ease-of-use barriers. Subsequent investment in and by the HCI community has yielded a wide variety of usability engineering and testing methods. It is now generally recognized that modern software and hardware cannot ignore usability. Potential users just will not adopt or use features that are difficult to use, and organizations will not deploy hardware and software that are difficult to manage.

Addressing these usability requirements has become an acknowledged part of most development methodologies. In software engineering, it has been adopted into process models such as the prototyping, iterative, and even spiral models.[10] Generally, these

---

[7]Helander, Martin G., Thomas K. Landauer, and Prasad V. Prabhu. 1997. *Handbook of Human-Computer Interaction, Second Edition*. New York: Elsevier.

[8]Baecker, Ronald M., William Buxton, Jonathan Grudin, and Saul Greenberg. 1995. *Readings in Human-Computer Interaction: Toward the Year 2000*. New York: Morgan Kaufmann.

[9]Karat, Clare-Marie, John Karat, and Carolyn Brodie. 2005. Usability Design and Evaluation for Privacy and Security Solutions. In L. Cranor and S. L. Garfinkel (eds), *Designing Secure Systems That People Can Use*, O'Reilly & Associates, Cambridge.

[10]Sommerville, Ian. 2001. *Software Engineering*. Reading, MA: Addison-Wesley.

recognize the need to iteratively design, develop, and test against real users in order to create usable systems. An excellent example of this process for a privacy mechanism can be seen in Cranor's implementation of Privacy Bird, which went through five iterations of development and evaluation.[11] Only through successive refinement can software engineers meet users' needs, capabilities, and expectations.

Privacy mechanisms are no exception. In many respects they can be treated as any other critical platform feature, and addressed with existing usability engineering methods. Karat, Brodie, and Karat[12] provide an excellent overview of these methods and their application for security and privacy. They also point out some key differences between privacy (and security) mechanisms and kinds of functional features with which usability engineering is more typically concerned, caveats which are worth paraphrasing and reflecting upon here:

1. *While valued, privacy is not the users' primary task*. We would just add that calling attention to privacy and making it an explicit *task* at any level can be problematic. For example, Cranor discusses users' difficulties in explicitly articulating their privacy preferences.[13] The goal with privacy, then, is often not so much to measure and refine task performance, as to refine task invisibility or lightweightness.
2. *Designs must encompass many different types of users*. Indeed, we devote a later section of this present chapter to a discussion of techniques for dealing with individual differences.
3. *Privacy raises the stakes.* Badly designed features can lead not only to user rejection and increased development costs, but also to potential injury (even bodily injury, in the case of stalking via location-tracking technologies).
4. *Systems must respond to the legal and regulatory environment*. We note that this places additional demands for specialized expertise on the makeup of usability engineering efforts, beyond their traditional interdisciplinary competencies.

Karat, Brodie, and Karat outline the various phases of system development and the types of methods appropriate to each. Rather than repeat that here, we conclude this section by emphasizing and introducing a number of general approaches from usability engineering and user-centered design of particular use to people seeking to understand a design domain in depth. These may be of particular use for new, "disruptive" technologies that do not yet have substantial deployments in the field.

---

[11]Cranor, Lorrie. 2005. Privacy Policies and Privacy Preferences. In L. Cranor and S. L. Garfinkel (eds), *Designing Secure Systems That People Can Use*, O'Reilly & Associates, Cambridge,

[12]Karat, Clare-Marie, John Karat, and Carolyn Brodie. 2005. Usability Design and Evaluation for Privacy and Security Solutions. In L. Cranor and S. L. Garfinkel (eds), *Designing Secure Systems That People Can Use*, O'Reilly & Associates, Cambridge.

[13]Cranor, Lorrie. 2005. Privacy Policies and Privacy Preferences. In L. Cranor and S. L. Garfinkel (eds), *Designing Secure Systems That People Can Use*, O'Reilly & Associates, Cambridge,

- Privacy is extremely contextual, based in the specifics of by who, for what, where, why, and when a system is being used. Understanding people's needs and attitudes, and developing the necessary empathy to understand the world from their point of view, is best derived by observing them "in the wild" and asking them open-ended questions. There really is no substitute for getting out into the field, and a number of more or less structured ethnographic methods have been developed. For example, Contextual Design[14] is a highly structured methodology to pull out the task requirements and context, that is, to go beyond the user interface and consider how users will use the privacy mechanisms in their tasks. Other approaches include discount ethnography[15] and rapid ethnography[16]; all of these seek to balance the valuable open-endedness and freedom of ethnographic investigations with practical requirements of timely return on research investments.
- Control over one's personal data is often very nuanced and unconscious in everyday life. In order to understand what people are doing, it is often necessary to get them talking; observation alone is not enough since it does not provide the subjective understanding of the situation. Nor are discussions of past behavior, since people are often not conscious of their actions and memory of what they did and why they did it can fade within minutes. For this reason, think-aloud protocols[17] were developed. In this methodology, users continuously describe their actions and reasons aloud. The researcher (or designer) may prompt the user from time to time to keep him talking, but the user provides a steady stream of reasons and subjective judgments. Over longer periods, related methodologies such as experience sampling[18] and diary keeping[19] may be useful.
- Systems need not be fully constructed in order to evaluate their usability. Both low-fidelity and high-fidelity prototypes can be used by potential users. An often fruitful method is the "Wizard of Oz" study. In a Wizard of Oz (named after the movie), the functionality of the system is simulated by people. For example, if the system requires the parsing of natural language text, this can be effectively done by a person

---

[14]Beyer, Hugh, and Karen Holtzblatt. 1997. *Contextual Design: A Customer-Centered Approach to Systems Designs.* San Francisco: Morgan Kaufmann.

[15]Hughes, John, Val King, Tom Rodden, and Hans Andersen. 1994. Moving Out from the Control Room: Ethnography in System Design. *Proceedings of the ACM Conference on Computer-Supported Cooperative Work (CSCW'94)* : 429-439.

[16]Millen, David R. 2000. Rapid ethnography: time deepening strategies for HCI field research. *Proceedings of the ACM Conference on Designing interactive systems: processes, practices, methods, and techniques* : 280-286.

[17]Lewis, Clayton. 1982. Using the 'Thinking Aloud' Method In Cognitive Interface Design. IBM Research Report, RC-9265.

Ericsson, K. Anders, and Herbert A. Simon. 1993. *Protocol Analysis: Verbal Reports as Data.* Cambridge: MIT Press.

[18]For example: Consolvo, Sunny, and Miriam Walker. 2003. Using the Experience Sampling Method to Evaluate Ubicomp Applications. *IEEE Pervasive Computing*, 2 (2) : 1536-1268.

[19]For example: Palen, Leysia, and Marilyn Salzman. 2002. Voice-mail diary studies for naturalistic data capture under mobile conditions. *Proceedings of the CSCW'2002* : 87-95.

who simulates the functioning, for example, of a natural language processing component of the potential system. In this way, designers can evaluate the adequacy of the system without constructing the system itself.

- The previous approaches – delving into users' worlds, helping them to articulate and self-reflect, and getting prototypes into their hands – can be combined, elaborated, and experimented with in almost limitless ways. Some particularly interesting hybrids include "experience prototyping," "bodystorming," and "informance".[20] These design techniques go beyond what is traditionally meant by usability engineering, but show promise for more adequately addressing the real-world nuances of domains like privacy.

None of these usability requirement gathering and usability evaluation techniques were constructed for privacy per se. However, because of the inherent complexity of privacy mechanisms, the large research stream about usability and user-centered design in HCI is potentially of considerable use.

The next research stream to be discussed considers how privacy mechanisms might be made more usable given the wide range of concerns and preferences that people have about their personal data.

## Computer-Supported Cooperative Work

An important stream of HCI research is Computer-Supported Cooperative Work (CSCW).[21] As mentioned, HCI began by examining largely single-user applications and systems. Starting in the late 1980s, CSCW began as a counter-effort to consider collaborative computer use. Although this subarea of HCI began in the consideration of cooperative or collaborative work, it quickly grew to include many different forms of coordination and social organization. It also grew to include many levels of analysis, from small groups to Internet-scale systems, and many types of activity, including work, entertainment, chat and other communication activities, and the like. Privacy is, in fact, the contrapositive of this research interest – it is what happens when many people can share data, some without their knowledge – and as such has become a research interest in its own right within CSCW.

While HCI overall began by drawing on cognitive psychology literature, CSCW's interest is in social interaction. As such, CSCW found its roots and assumptions largely in micro-sociology, as well to a lesser extent in social psychology and cognitive anthropology. This background is not only important to understanding current CSCW research but it is also critical in understanding privacy overall. For that reason, we next survey some of the key social theorists. (We follow this with an overview of the current

---

[20]Buchenau, Marion, and Jane Fulton Suri. 2000. Experience prototyping. *Proceedings of the Conference on Designing interactive systems: processes, practices, methods, and techniques* : 424-433.

[21]Grudin, Jonathan. 1994. Computer-supported cooperative work: History and focus. *IEEE Computer*, 27 (5) : 19-26.

Olson, Gary M., and Judith S. Olson. 1997. Research on Computer Supported Cooperative Work. In M. Helander (eds), *Handbook of Human Computer Interaction*, Elsever, Amsterdam, in press.

CSCW literature appropriate to privacy mechanisms.) In many ways, these theorists' views have become almost assumptions within CSCW, and many CSCW studies have borne out their theories. The theorists' views most important to a discussion of privacy include:

- As people interested in privacy are aware, people have very nuanced views of their interactions with other people and find it problematic when those social interactions are constrained.[22] They handle this nuance with agility and contextually.[23]
- Goffman[24] noted people present a "face" to others. Goffman, fascinated by spies and scam artists, proposed that everyone presents bits and pieces of themselves as socially appropriate to the other, and in fact, may wish to present themselves differently depending on the circumstances. A person may present himself as a loyal employee to his supervisor and a job seeker to another company. People find it very disconcerting when that capability is removed.
- Garfinkel[25], in his examination of how people make sense of their everyday worlds, showed that people find it disconcerting when what they believe to be their everyday "normal" world is disrupted. Some people may even become violently angry when they believe the rules of conduct or "normal" behavior are violated.

Privacy mechanisms, in specific, suffer from these issues. People have extremely nuanced views of other people (and groups, companies, and institutions), and want to safeguard their ability to properly present themselves to those others. At the same time, they will find it very difficult when those modes of presenting themselves change, or when the "rules" about their privacy and safeguards change.

Drawing on these theorists, CSCW research relevant to privacy can be roughly divided into three categories: media space applications, other collaborative applications with privacy concerns, and studies discussing privacy in relation to awareness. CSCW interest in shared spaces, linked geographically through audio and video, goes back to experiments in the early 1990s.[26] These shared spaces, or media spaces, could be either a special display (for example, a video wall linking two lunchrooms) or between offices.

---

[22]Strauss, Anselm L. 1993. *Continual Permutations of Action*. New York: Aldine de Gruyter.

[23]Suchman, Lucy A. 1987. *Plans and Situated Actions: The Problem of Human-Computer Communication*. New York: Cambridge University Press.

[24]Goffman, Erving. 1961. *The Presentation of Self in Everyday Life*. New York: Anchor-Doubleday.

[25]Garfinkel, Harold. 1967. *Studies in Ethnomethodology*. Englewood Cliffs, NJ: Prentice-Hall.

[26]For example: Dourish, Paul, and Sara Bly. 1992. Portholes: Supporting Awareness in a Distributed Work Group. *Proceedings of the ACM CHI'92 Conference on Human Factors in Computing Systems* : 541-547.

Buxton, William. 1993. Telepresence: Integrating Shared Task and Person Spaces. In R. M. Baecker (eds), *Readings in Groupware and Computer-Supported Cooperative Work*, Morgan-Kaufmann, San Mateo, CA, 816-822.

Bly, Sara A., Steve R. Harrison, and Susan Irwin. 1993. Media Spaces: Bringing People Together in a Video, Audio, and Computing Environment. *Communications of the ACM*, 36 (1) : 28-47.)

Media spaces had obvious privacy problems. In one important study[27], one of the authors found that she forgot that their camera was on, and began to change clothes. Other authors have reported similar events. These spaces began a significant interest in privacy in CSCW.

Other applications raised similar privacy concerns. Palen[28] explored the issues with shared calendars and sharing information about users' schedules with co-workers, managers, and employees. For example, Palen noted that some workers used viewing their supervisor's open calendars to determine whether layoffs were likely, a move that might not have been in the company's interest. Other work on shared or public displays has raised concerns about automatically generated views or making information public. Finally, allowing people to view one another's temporal information, as in when people are available for communication, also raises obvious privacy concerns.[29]

These privacy problems have been analyzed in a series of papers that discuss the tradeoffs between *awareness* and privacy. Awareness is knowing what others are doing or even that they are around. First raised in media space studies[30] and other shared work investigations[31], awareness is a critical issue in distributed, collaborative applications – one needs to know what other people are doing in the shared space. Hudson and Smith[32] went on to discuss the fundamental tradeoff between awareness and privacy. In their view, awareness requires the release of personal information; this necessitates the disruption of privacy or at least required one's attention to controlling the release of personal data. They proposed a number of interesting technical solutions to solving the privacy-awareness tradeoff. Their video solution allowed cameras to provide awareness of a presence, but the blurred image did not allow the viewer to see details.[33] Their audio solution allowed one to hear voices in a media space, but not make out the exact words.

---

[27]Dourish, Paul, Annette Adler, Victoria Bellotti, and Austin Henderson. 1996. Your Place or Mine? Learning from Long-Term Use of Audio-Video Communication. *Computer Supported Cooperative Work*, 5 (1) : 33-62.

[28]Palen, Leysia. 1999. Social, individual and technological issues for groupware calendar systems. *Proceedings of the ACM Conference on Human Factors in Computing Systems* : 17-24.

[29] Begole, James Bo, Nicholas E. Matsakis, and John C. Tang. 2004. Lilsys: Sensing Unavailability. *Proceedings of the ACM conference on Computer supported cooperative work* : 511-514.

[30]For example: Dourish, Paul, and Victoria Bellotti. 1992. Awareness and Coordination in Shared Workspaces. *Proceedings of the Conference on Computer-Supported Cooperative Work (CSCW'92)* : 107-114.

[31]For example: Heath, Christian, and Paul Luff. 1992. Collaboration and Control: Crisis Management and Multimedia Technology in London Underground Line Control Rooms. *Computer Supported Cooperative Work Journal*, 1 (1) : 69-94.

[32]Hudson, Scott E., and Ian Smith. 1996. Techniques for Addressing Fundamental Privacy and Disruption Tradeoffs in Awareness Support Systems. *Proceedings of the ACM Conference on Computer-Supported Cooperative Work (CSCW'96)* : 248-257.

[33] This idea was also considered in Boyle, Michael, Christopher Edwards, and Saul Greenberg. 2000. The effects of filtered video on awareness and privacy. *Proceedings of the ACM Conference on Computer supported Cooperative Work* : 1-10..

Both of their solutions were ingenious. Neither solution required a user's attention, and yet particularly egregious problems, such as seeing too much or overhearing private conversations, were eliminated for workplace environments (See Neustaedter, Greenberg, and Boyle for a caution for home environments.)

Work on privacy continues within CSCW. Recently, Dourish and Palen[34] published a work pointing out that privacy is a dynamic, dialectic process. Based on the work of Altman[35], Dourish and Palen analyze the relational nature of privacy. Ackerman[36] has discussed the difficulty of privacy, and has suggested that because of the relational, nuanced, and situated complexity of privacy issues for many people, there is likely to be a gap between what we know we must do socially and what we know how to do technically. He calls this the social-technical gap, and sees it as a major stumbling block for building effective user-centered controls for privacy mechanisms. And finally, Friedman[37] is examining design methodologies that can include value-driven issues such as privacy.

## Individual differences

Users differ widely in their privacy concerns. We know from the research literature that individuals do not view "privacy" uniformly, even in e-commerce. Types of concerns and degree of concern segment the population. First, people have differing types of concerns. Culnan and Armstrong[38] make the argument that people have two kinds of privacy concerns. First, they are concerned over unauthorized others accessing their personal data because of security breaches or the lack of internal controls. Second, people are concerned about the risk of secondary use; that is, the reuse of their personal data for unrelated purposes without their consent. This includes sharing with third parties who were not part of the original transaction. It also includes the aggregation of personal data to create a profile. Smith, Milberg, and Burke[39] raise two additional concerns: People have a generalized anxiety about personal data being collected, and people are also concerned over their inability to correct any errors.

---

[34]Palen, Leysia, and Paul Dourish. 2003. Unpacking "privacy" for a networked world. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)* : 129-136.

[35]Altman, Irving. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*. Monterey, CA: Brooks/Cole Publishing.

[36]Ackerman, Mark S. 2000. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human-Computer Interaction*, 15 (2-3) : 179-204.

[37]For example: Millett, Lynette I., Batya Friedman, and Edward Felten. 2001. Cookies and Web browser design: toward realizing informed consent online. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)* : 46-52.

[38]Culnan, Mary J., and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10 (1) : 104-115.

[39]Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, June : 167-196.

People also differ in their level of concern. The research literature generally describes a general anxiety and its extent, but there is some research providing more detail. A persistent finding is that it is useful to consider US consumers not as one homogenous group. Westin[40] found three separate groups: the marginally concerned, privacy fundamentalists, and the pragmatic majority. The groups differ significantly in their privacy preferences and attitudes. The marginally concerned group is mostly indifferent to privacy concerns; privacy fundamentalists, on the other hand, are quite uncompromising about their privacy. The majority of the US population, however, are members of the pragmatic majority. The pragmatic majority are concerned about their privacy, but are willing to trade personal data for some benefit (e.g., customer service).

These groupings have been consistent across studies.[41] (Spiekermann, Grosslags, and Berendt divided the pragmatics into those who were concerned with revealing their identity and those who were more concerned about making their personal profiles available.) Estimates of these groups' sizes differ, and they appear to be changing over time. Westin found population estimates shown in Table 1; note that Westin 2003 is a study after 9/11. Spiekermann et al. noted a larger group of privacy fundamentalists and fewer marginally concerned in Germany. It should be noted that, despite these groupings, consumers still want adequate measures to protect their information from inappropriate sale, accidental leakage or loss, and deliberate attack.[42] Indeed, in Ackerman, Cranor, and Reagle[43], the concerns of pragmatists were often significantly reduced by the presence of privacy protection measures such as privacy laws or privacy policies on Web sites.

| | privacy fundamentalists | marginally concerned | pragmatic majority |
|---|---|---|---|
| Westin 1995 | 25% | 20% | 55% |
| Westin 2000 | 25% | 12% | 63% |
| Westin 2003 | 37% | 11% | 52% |

[40]Westin, Alan F. 1991. *Harris-Equifax Consumer Privacy Survey 1991*. Atlanta: Equifax, Inc.

[41]For example: Ackerman, Mark S., Lorrie Cranor, and Joseph Reagle. 1999. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. *Proceedings of the ACM Conference in Electronic Commerce* : 1-8.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. *Proceedings of the ACM Conference on Electronic Commerce* : 38-46.

[42]Dhillon, Gurpreet S., and Trevort T. Moores. 2001. Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal*, 14 (4) : 33-37.

[43]Ackerman, Mark S., Lorrie Cranor, and Joseph Reagle. 1999. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. *Proceedings of the ACM Conference in Electronic Commerce* : 1-8.

*Table 1: population estimates, by privacy cluster.*[44]

Given this diversity in how users view privacy, how might one design for these differences among users' capabilities, concerns, and preferences? An old research theme in HCI is that of individual differences. Experimental and cognitive psychology, as literatures, have largely ignored differences between subjects, seeing them as part of experimental error. As well, as Egan[45] notes, "Differences among users have not been a major concern of commercial computer interface designers. (p. 543)" However, HCI's heritage in man-machine interfaces (human factors) led HCI to appreciate how people varied. Human factors had found this critical: When constructing airplane cockpits, industrial lighting, or even office chairs, differences between individuals can be critical for safety, comfort, and usability. This concern from human factors led over into user interfaces and HCI research.

Egan[46] summarizes much of the work in early HCI about individual differences. It should be noted that this research theme is largely moribund in HCI.[47] The later volume of the Handbook of Human-Computer Interaction[48], published in 1997, does not have a similar chapter. However, rekindling this research stream is likely to be of help to privacy and similar mechanisms.

The interest in Egan's chapter, as well as most of the individual differences research, was to determine the source of efficiencies and errors in using computer systems. The goal was to find ways to help users more effectively use their task knowledge as well as to reduce errors. As he notes, there are huge variances among users' performance (occasionally 20:1), much more extreme than among workers performing tasks (at most 2:1). Users have, if anything, even wider variance when considering privacy. One can see that people vary not only in their system performance, as well as their understanding of the task and its implications for privacy. All of these differences, as well as their attitudes, must be considered when constructing privacy mechanisms, and as HCI found, several standard techniques can be used.

These approaches to accommodating user differences should be of considerable interest to those constructing or researching privacy mechanisms. The approaches described by

---

[44]Westin, Alan. 2003. *http://www.harrisinteractive.com/advantages/pubs/DNC_AlanWestinConsumersPrivacyandSurveyResearch.pdf.*

[45]Egan, Dennis E. 1988. Individual Differences in Human-Computer Interaction. In M. Helander (eds), *Handbook of Human-Computer Interaction*, North-Holland, New York, NY, 543-568.

[46]Egan, Dennis E. 1988. Individual Differences in Human-Computer Interaction. In M. Helander (eds), *Handbook of Human-Computer Interaction*, North-Holland, New York, NY, 543-568.

[47] But see Dillon, Andrew, and Charles Watson. 1996. User analysis in HCI: the historical lesson from individual differences research. *International Journal of Human-Computer Studies*, 45 (6) : 619-637.

[48]Helander, Martin G., Thomas K. Landauer, and Prasad V. Prabhu. 1997. *Handbook of Human-Computer Interaction, Second Edition*. New York: Elsevier.

Egan are still the predominant methods in HCI research and practice for handling diversity, and they are of direct relevance to privacy mechanisms. These approaches are:

- *Constructing better interfaces*. As Egan stated, "This approach is similar to standard human-interface design, except that it is shaped by a concern for the variability among users. (p. 559)."[49] This is particularly important for systems where people are not expert users and where they will remain "permanent casual users."

  Redesigning interfaces and systems so as to reduce usability problems is a laudable goal. Yet, because of the complexity of privacy concerns for users, it is unlikely that a "one size fits all" approach will work adequately.[50] The concomitant possibility of constructing software that has all potential privacy functionality for a task (like the solution adopted by some word processors and office applications) may not work with privacy concerns or may be too complex for users, since the functionality is likely to cut across many tasks, systems, and applications.

- *Clustering users*. This approach advocates accommodating user differences by finding a set of user clusters and then interacting with the users through those classifications. This can be done in several different ways. Egan viewed it largely as a question of developing different interfaces. One could also have different dialog or interaction patterns with different user classes. More currently, one might treat these differing clusters of users differently. As Egan states, "Identical actions from two different users may be treated quite differently if the users have been classified as different prototypes [classes] (p. 560)".[51]

  Indeed, work on several problems shows the analytical power in examining user clusters. One set of papers examines default settings ().[52] Most users not only do not program their systems, they do not even customize them or change the default settings. [53]

[49]Egan, Dennis E. 1988. Individual Differences in Human-Computer Interaction. In M. Helander (eds), *Handbook of Human-Computer Interaction*, North-Holland, New York, NY, 543-568.

[50]Ackerman, Mark S. 2000. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human-Computer Interaction*, 15 (2-3) : 179-204.

[51]Egan, Dennis E. 1988. Individual Differences in Human-Computer Interaction. In M. Helander (eds), *Handbook of Human-Computer Interaction*, North-Holland, New York, NY, 543-568.

[52]Mackay, Wendy E., Thomas W. Malone, Kevin Crowston, Ramana Rao, David Rosenblitt, and Stuart K. Card. 1989. How Do Experienced Information Lens Users Use Rules? In (eds), *Proceedings of ACM CHI'89 Conference on Human Factors in Computing Systems*, 211-216.

Mackay, Wendy E. 1991. Triggers and Barriers to Customizing Software. In (eds), *Proceedings of ACM CHI'91 Conference on Human Factors in Computing Systems*, 153-160.

Grudin, Jonathan. 2004. Managerial Use and Emerging Norms: Effects of Activity Patterns on Software Design and Deployment. *Proceedings of the Hawaii International Conference on System Sciences 37*

[53]Mackay, Wendy E. 1990. Patterns of Sharing Customizable Software. In (eds), *Proceedings of ACM CSCW'90 Conference on Computer-Supported Cooperative Work*, 209-221.

Another set of research shows that different groups have different mental models or technology frames.[54] Orlikowski[55], in her study of a collaborative work system, showed that administrative personnel, managers, front-line consultants, and information technology staff all brought differing incentives and disincentives, reward and compensation expectations, and goals. For example, front-line consultants could not bill to learn the system, whereas information technology workers wanted to know as much about the system as possible. Similarly, privacy mechanisms will be used very differently not only by people with differing assumptions about power and control, the efficacy of regulation and law, and the benign intent of companies. Finding suitable user clusters will be important, but may be challenging, especially for members of the pragmatic majority. In some situations, however, it may be possible to teach users and consumers new technology frames. Orlikowski noted the importance of training.

These two lines of inquiry have led to discussions of creating specific default and other settings for varying user clusters. Grudin[56] suggested defaults for office applications, where different groups of people (managers, administrative assistants, and knowledge workers) use the systems very differently. For privacy, while the pragmatics are a large and highly differentiated group in their everyday, contextualized preferences, it may be quite possible to treat privacy fundamentalists and the marginally concerned as user clusters. By doing so, it may be possible to create usable privacy mechanisms for at least these groups (which may be over a majority of the population). Very recently, Olson, Grudin, and Horvitz[57] explored clustering in privacy preferences. While their work is still preliminary, it suggests that there are key classes of recipients and data. While people vary overall, these classes of recipients and data may remain relatively constant.

- *Adaptive systems.* These systems prevent user errors by helping users. Carroll, in a line of work,[58] promoted "training wheels" interfaces with reduced functionality to as to avoid errors from complex interactions with the system. Similarly, critics are

54

Orlikowski, Wanda J. 1992. Learning from Notes: Organizational Issues in Groupware Implementation. *Proceedings of the Computer Supported Cooperative Work (CSCW'92)* : 362-369.

Orlikowski, Wanda J. 1992. The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science*, 3 (3) : 398-427.

[55]Orlikowski, Wanda J. 1992. Learning from Notes: Organizational Issues in Groupware Implementation. *Proceedings of the Computer Supported Cooperative Work (CSCW'92)* : 362-369.

[56]Grudin, Jonathan. 2004. Managerial Use and Emerging Norms: Effects of Activity Patterns on Software Design and Deployment. *Proceedings of the Hawaii International Conference on System Sciences 37*

[57]Olson, Judith S., Jonathan Grudin, and Eric Horvitz. 2004. Toward Understanding Preferences for Sharing and Privacy. Microsoft Research Technical Report 2004-138.

[58]For example: Carroll, John M., and C. Carrithers. 1984. Training Wheels in a User Interface. *Communications of the ACM*, 27 (8) : 800-806.

interface agents that help users avoid mistakes by noting when there are problems.[59] In Fischer and Lemke[60], the critics let the users (who were kitchen designers) know when they had made a mistake, such as placing an appliance in front of a door. Ackerman and Cranor[61] used critics for helping users with their privacy on the Web. Their Privacy Critics system alerted the user when, for example, the user might be violating their own privacy or when sites might be problematic.

- *Automated "Mastery Learning"*. HCI has had a large number of studies on training and documentation. Egan promoted using automatic training, such as tutors, to help users gain the expertise necessary to effectively use systems. Many studies[62] have noted the use of training to facilitate changing or expanding users' mental models of the system and potential tasks. To our knowledge, no such tutoring or training system has been constructed for privacy, although one would be clearly useful.

A fifth approach has also arisen. It follows from the first two approaches:

- *Tailorable systems*. Another approach is to have users tailor or customize the systems to fit their needs. Customizing usually refers to changing the surface interfaces of a system; tailoring usually refers to deeper changes to the functionality of an application.[63] In this approach, the designer includes large amounts of functionality, most of which any given user will not use. Unlike robust interfaces, which present “one size fits all” interfaces, tailorable systems allow users to pick and choose their functionality. Information technology personnel, users with computer expertise (called gardeners in Nardi[64]), or even end-users customize and tailor the systems to create new or specialized applications.

  Much of this work has appeared in the context of group applications (see above), because of the need to fulfill the needs of many users simultaneously. Discussions of

[59]Fischer, Gerhard, Andreas C. Lemke, Thomas Mastaglio, and Anders I. Morch. 1990. Using Critics to Empower Users. In (eds), *Proceedings of ACM CHI'90 Conference on Human Factors in Computing Systems*, 337-347.

[60]Fischer, Gerhard, and Andreas C. Lemke. 1988. Construction Kits and Design Environments: Steps Toward Human Problem-Domain Communication. *Human-Computer Interaction*, 3 (3) : 179-222.

[61]Ackerman, Mark S., and Lorrie Cranor. 1999. Privacy Critics: UI Components to Safeguard Users' Privacy. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'99)* : 258-259.

[62]For example: Orlikowski, Wanda J. 1992. Learning from Notes: Organizational Issues in Groupware Implementation. *Proceedings of the Computer Supported Cooperative Work (CSCW'92)* : 362-369.

[63]Hummes, Jakob, and Bernard Merialdo. 2000. Design of Extensible Component-Based Groupware. *Computer Supported Cooperative Work Journal*, 9 (1) : 53-74.

[64]Nardi, Bonnie. 1993. *A Small Matter of Programming: Perspectives on End User Computing*. Cambridge: MIT Press.

the organizational and social requirements can be found in Trigg and Bodker.[65] Their major findings include the necessity for having both people with task knowledge and local technical support to help the tailoring process. Discussions of potential system architectures and requirements can be found in Hummes and Merialdo[66] and Dourish and Edwards.[67]

In summary, then, HCI has considerable experience with dealing with individual differences. In one approach suitable to privacy mechanisms, it has been found valuable to cluster users, and then to present different interfaces or functionality to those users. Another approach is to allow users to tailor the systems to their own needs; however, this often requires that they obtain tailoring help from others. And last, two intelligent augmentations have been found to be helpful in the HCI literature – mechanisms to help users prevent errors as well as mechanisms to help tutor the users about, in this case, privacy.

The idea of designing for individual differences also has a downside that is important to keep in mind: the potential for amplifying power imbalances and decreasing fairness. By classifying someone as a privacy fundamentalist, say, a system could decide he is too much trouble and put up barriers to discourage use. Conversely, unscrupulous designers could segment users in order to seek out novices or the marginally concerned, not to offer targeted assistance, but for relatively easy exploitation. These issues are not restricted to privacy, as any system that discriminates between users opens itself to the question of whether this discrimination is unfair (or paternalistic, deindividualizing, or otherwise unwarranted). While important to acknowledge and guard against, in terms of actual effects or perception, this is not to say that an individual differences approach is to be avoided – only to be used with caution.

## Ubiquitous Computing (Ubicomp)

There is currently considerable interest in ubiquitous and pervasive computing in HCI.[68] In these architectures, one might have hundreds or even thousands of sensors and other computational devices spread out through a room, building, or other environment. People would be wearing them, carrying them, or might even have them embedded. HCI and ubicomp are not identical areas of computer science, but there is overlap in research. In

[65]Trigg, Randall H., and Susanne Bodker. 1994. From Implementation to Design: Tailoring and the Emergence of Systematization in CSCW. *Proceedings of the ACM Conference on Computer-Supported Cooperative Work* : 45-54.

[66]Hummes, Jakob, and Bernard Merialdo. 2000. Design of Extensible Component-Based Groupware. *Computer Supported Cooperative Work Journal*, 9 (1) : 53-74.

[67]Dourish, Paul, and W. Keith Edwards. 2000. A Tale of Two Toolkits: Relating Infrastructure and Use in Flexible CSCW Toolkits. *Computer Supported Cooperative Work Journal*, 9 (1) : 33-51.

[68]For an overview, see Abowd, Gregory D., and Elizabeth D. Mynatt. 2000. Charting past, present, and future research in ubiquitous computing. *ACM Transactions on Computer-Human Interaction*, 7 (1) : 29-58..

particular, HCI researchers are very interested in augmented reality applications (where the digital world augments the physical), sensor-based entertainment (such as geo-games), and user-centered interfaces to ubicomp rooms.

There are significant privacy concerns for ubiquitous computing (ubicomp) environments. Obviously, location sensors can track individuals through an environment. Sensor aggregation could tell a large amount about what any given individual might be doing. Large amounts of seemingly personal data could be collected without notice or consent of an environment's users.

Recently, several studies have specifically examined privacy in ubicomp environments. In an ethnographic field study, Beckwith[69] found that workers and elderly residents in a sensor-network equipped assisted-care facility had very limited understanding of the potential privacy risks of the technology. They instead trusted that the system was benign and perceiving the privacy risks to be minimal. Without understanding, informed consent is very difficult. As with work in media spaces[70], unobtrusive interfaces that encourage users to forget they are being recorded or tracked bring benefits in ease-of-use but also risks to users.

Other work considers methodologies for designing for privacy in these new environments. Langheinrich[71], drawing upon the European Union's privacy directive of 1995, identifies seven guiding principles for ubicomp designs: notice, choice and consent, anonymity and pseudonymity, proximity and locality, adequate security, and access and recourse. This work calls attention to legal frameworks not just as requirements to be met, but also as sources of design inspiration and insight. Hong et al.[72] proposes a methodology for prototyping ubicomp applications involving the development of a privacy risk model (though a kind of heuristic evaluation, combined with validation through user testing). Lederer et al.[73] also provides design guidelines for privacy.

---

[69]Beckwith, R. 2003. Designing for ubiquity: the perception of privacy. *IEEE Pervasive Computing*, 2 (2) : 40-46.

[70]For example: Ackerman, Mark S., Debby Hindus, Scott D. Mainwaring, and Brian Starr. 1997. Hanging on the 'wire: A field study of an audio-only media space. *ACM Transactions on Computer-Human Interaction*, 4 (1) : 39-66.

Dourish, Paul, Annette Adler, Victoria Bellotti, and Austin Henderson. 1996. Your Place or Mine? Learning from Long-Term Use of Audio-Video Communication. *Computer Supported Cooperative Work*, 5 (1) : 33-62.

[71]Langheinrich, Marc. 2001. Privacy by design - Principles of privacy-aware ubiquitous systems. *Proceedings of the Ubicomp 2001* : 273-291.

[72]Hong, Jason I., Jennifer D. Ng, Scott Lederer, and James A. Landay. 2004. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. *Proceedings of the ACM Conference on Designing Interactive Systems* : 91-100.

[73]Lederer, Scott, Jason I. Hong, Anind K. Dey, and James A. Landay. 2004. Personal Privacy through Understanding and Action: Five Pitfalls for Designers. *Personal and Ubiquitous Computing*, 8 (6) : 440-454.

Finally, Hong and Landay[74] examine the system issues. Their Confab system provides a middleware layer for building ubicomp applications. Combining a blackboard and dataflow architecture, Confab allows users to publish and services to request data with strong privacy controls. Users can place privacy tags on all data that control access within a Confab infospace and provide hints about how the data are to be used outside the Confab system. In addition to customizable privacy mechanisms, Confab also includes extension mechanisms, currently about location awareness.

Ubicomp research is just beginning, and over time, we expect this to provide considerable feedback to privacy mechanisms overall.

# Conclusions

In this chapter, we presented a range of HCI research that we believe can be of help to those designing privacy mechanisms. These were usability evaluations and requirements gathering, including the large range of HCI methods for incorporating users and users' viewpoints in the process; collaborative views of information and activity, including many systems and applications as well as a range of social analyses that promote a detailed, situated view of privacy; handling diversity and difference among users, including the HCI approaches to this problem; and, new approaches to new computational environments, including studies and systems for pervasive environments.

We note in passing that HCI could profit by considering privacy more fully. The direction of research should not be one-way. Cross-cultural studies of privacy could inform the nascent interest in HCI in cross-cultural interfaces and coordination. Increased understanding of the diversity and complexity of user preferences, and potential clusterings, is providing new impetus for HCI research on individual differences. As well, considering visualizations and intelligent tutoring systems for privacy, in a range of applications and tasks, could germinate new emphases in HCI. We hope that HCI work grows to consider these and other aspects of privacy needs.

Privacy in digital environments is likely to remain a critical issue for the foreseeable future. As it directly engages aspects of user control and power, it is central to the concerns of HCI. We fully expect the two areas of interest – HCI and privacy – to remain closely interlocked in interest and need.

# Sidebar – A CSCW Research Study: Thunderwire

`[To be inserted after the CSCW section.]`

Thunderwire was an experimental audio-only media space prototype developed at Interval Research. It provided a kind of "party line" shared audio connection that was

[74]Hong, Jason I., and James A. Landay. 2004. An architecture for privacy-sensitive ubiquitous computing. *Proceedings of the 2nd international conference on Mobile systems, applications, and services* : 177-189.

continuously available to a small, fixed group of spatially distributed users. Thunderwire had an intentionally minimalist interface (to see how simple such interfaces could be while still usable): basically an on/off switch. When on, microphones at fed local audio into the party line and lit a red "on the air" light to notify the user (and any passersby). Off deactivated all of these. Its users were a video analysis and analysis tool-building team who routinely worked with audio, facilitating the addition of Thunderwire to their work practices. Their manager wished to use the system as an awareness technology, to more tightly integrate the team across locations within two buildings.

The field study lasted two months and consisted of 9 users. Overall, the success of the Thunderwire experiment was mixed. But for a small core of habitual users, it became a valued and enlivening aspect of their workplace, a predominantly social medium allowing for intermittent chat among friends. These benefits came with privacy problems, chiefly the inability to tell who at any given time was present on the party line, as well as recurring problems with leaving the system on by mistake and unintentionally broadcasting phone conversations, bodily noises, and other distractions. Unintentional broadcasting was a serious issue; similar to other media space studies, participants forgot that they were part of a live, shared space. Of particular interest was how the group developed informal social norms about how the system was and was not to be used, as well as how exceptions were to be handled. In this way, the participants were able to make the system usable for themselves.

The researchers used multiple methods to collect data about the system over a two-month study period. A central server continuously logged when each user connected or disconnected. Two weeks of audio activity were recorded (with all users' knowledge and permission). An outside researcher (the first author) was contracted to study the system. He observed their work, and he interviewed the users before, during, and after the system deployment. He and his students also transcribed and analyzed 18 hours of the system's audio, which captured the nuances of actual system use.. Having an "outsider" as principal investigator was important to ensure the confidentiality of the people's data and encourage openness on the part of interviewees; it also to bring new perspectives and disciplinary backgrounds to the research team.

For a full analysis, see: Ackerman, Mark S., Debby Hindus, Scott D. Mainwaring, and Brian Starr. 1997. Hanging on the 'wire: A field study of an audio-only media space. *ACM Transactions on Computer-Human Interaction*, 4 (1) : 39-66.

# Biographies

Mark S. Ackerman is an Associate Professor of Electrical Engineering and Computer Science and of Information at the University of Michigan. He has published extensively on a number of Human-Computer Interaction topics, including Computer-Supported Cooperative Work, information access, collaborative memory systems, and privacy.

Scott D. Mainwaring is a Senior Researcher in the People and Practices Research Lab at Intel Research. His research interests include design ethnography, home environments, human relationship to infrastructure, and the community, trust, and privacy implications of ubiquitous computing.