Chapter 7
Privacy Factors in Video-based Media Spaces

Michael Boyle, Carman Neustaedter, and Saul Greenberg

Abstract Media space research is accompanied by a long-standing debate on the value of awareness leading to casual interaction *vs*. its potential for intended or unintended privacy invasion. This is not just a matter of technology: the trade-off between the two depends very much on the social makeup of the people using the space, how cameras are actually situated, the kinds of activities that typically happen in the space, and so on. This chapter offers a framework—a descriptive theory—that defines how one can think of privacy while analyzing media spaces and their expected or actual use. The framework outlines existing perspectives on privacy and then decomposes privacy into three normative controls for regulating interpersonal boundaries in an embodied dialectic: solitude, confidentiality and autonomy. By considering the nuances of these controls, this theory yields a powerful vocabulary of terms that disambiguate the many interrelated and subtle meanings of "privacy."

M. Boyle
SMART Technologies, ULC

C. Neustaedter
Kodak Research Labs

S. Greenberg
University of Calgary

Table 1 Vocabulary terms for SOLITUDE.

1. SOLITUDE

a) Physical Dimensions	b) Psychological Dimensions	c) Presentation Dimensions
i) Interpersonal Distance (1) isolation to crowding ii) Attention (1) focus to periphery	i) Interaction to Withdrawal (1) anonymity and reserve to intimacy ii) Escape (1) refuge (2) fantasy	i) High-level Awareness (1) availability (2) accessibility ii) Distraction (1) relevance (2) salience

Table 2 Vocabulary terms for CONFIDENTIALITY.

2. CONFIDENTIALITY

a) Information Channels	b) Information Characteristics	c) Information Operations
i) Medium (1) aural (2) visual (3) numeric (4) textual ii) Processing (1) sampling (2) interpolation (3) aggregation (4) inference iii) Topic (1) information about the self (2) personally identifying information (3) activities (4) whereabouts (5) encounters (6) utterances (7) actions (8) relationships	i) Basic Characteristics (1) sensitivity (2) persistence (3) transitivity ii) Fidelity (1) precision (2) accuracy (3) misinformation (4) disinformation iii) Certainty (1) plausible deniability (2) ambiguity	i) Basic Operations (1) capture (2) archival (3) edit ii) Intention / Use (1) accountability (2) misappropriation (3) misuse iii)Scrutiny (1) surreptitious surveillance (2) analysis

Table 3. Vocabulary terms for AUTONOMY.

3. AUTONOMY

a) Social Constructions of the Self
   - i) Front
     - (1) identity
     - (2) digital persona
     - (3) appearance
     - (4) impression
     - (5) personal space
   - ii) Back
     - (1) flaws
     - (2) deviance*
     - (3) idealisations
   - iii) Signifiers*
     - (1) territory
     - (2) props
     - (3) costumes
   - iv) Harms
     - (1) aesthetic
     - (2) strategic

b) Social Environment
   - i) Social relationships
     - (1) roles
     - (2) power
     - (3) obligations
     - (4) status divisions
     - (5) trust
   - ii) Norms
     - (1) expectations
     - (2) preferences
     - (3) social acceptability
     - (4) conformance
     - (5) deviance
     - (6) place

Table 4. Vocabulary terms for MECHANICS OF PRIVACY.

4. MECHANICS OF PRIVACY

a) Boundaries i) disclosure ii) temporal iii) spatial iv) identity	b) Process Characteristics i) dialectic ii) dynamic iii) regulation iv) cooperation	c) Violations i) risk ii) possibility iii) probability iv) severity v) threat
d) Behavioural and Cognitive Phenomena i) self-appropriation ii) genres of disclosure iii) policing iv) reprimand v) reward vi) risk/reward trade-off vii) disclosure boundary tension viii) disinformation* ix) reserve* x) Signifiers* (1) implicit (2) explicit	e) Environmental Support i) situated action ii) reflexive interpretability of action iii) constraints iv) transitions v) choice vi) reciprocity vii) liberty viii) refuge* ix) Embodiments (1) rich to impoverished x) Cues (1) feedback (2) feed-through	

Table 5. Vocabulary terms for COMPUTERS AND PRIVACY.

5. COMPUTERS AND PRIVACY

a) Support Methods
   - i) computer security
   - ii) cryptography
   - iii) pseudonymity
   - iv) access control
     - (1) authentication
     - (2) authorisation
   - v) Content Control
     - (1) distortion filtration
     - (2) publication filtration
   - vi) Reliability
     - (1) data integrity
     - (2) process integrity
     - (3) stability

b) Problems
   - i) inadvertent privacy infractions
   - ii) apprehension
   - iii) resentment
   - iv) the four 'D's : decontextualisation, disembodiment, dissociation, desituated action
   - v) role conflict
   - vi) deliberate abuse
     - (1) misappropriation
     - (2) misuse
     - (3) identity theft
     - (4) impersonation

c) User Interface Issues
   - i) degrees of temporal/ spatial freedom for information access
   - ii) risk/reward disparity
   - iii) Feedback and Control
     - (1) believ-ability
     - (2) socially natural qualities
     - (3) utility of privacy counter-measures
   - iv) Effort
     - (1) cognitive
     - (2) physical
     - (2) lightweight control
   - v) Control Granularity
     - (1) fine- to coarse-grained

1 Introduction

Video media spaces (VMS) connect small groups of distance-separated collaborators with always-on or always-available video channels. Via these video channels, people gain informal awareness of others' presence and their activities. This awareness permits fine-grained coordination of frequent, light-weight casual interactions. While video media spaces are a promising way to increase group interaction, they are perceived by users and non-users alike to be privacy invasive and privacy insensitive, e.g., Gaver et al (1992), Bellotti & Sellen (1993), Lee et al (1997). They permit privacy violations that range from subtle to obvious and from inconsequential to intolerable. Even early media spaces proponents, while enthusiastic about the technology, raised concerns about privacy and its potential for sociological and psychological impact. This is evident in the various anecdotes presented in this book from early media space researchers (and users) such as Victoria Bellotti, Bill Buxton, and Deborah Tatar.

Yet, what do we mean when we say "privacy"? If a media space person is concerned about their privacy, do they mean they are worried about others spying on them (surveillance), or being caught by one's companions in an embarrassing act, or theft of their video image, or that they would be continually interrupted, or that others would masquerade as them? In reality, privacy is a multifaceted thing, connected with much of daily life and highly dependant on context. Perhaps because of this, privacy has been given considerable diverse treatment by hundreds of authors in scientific, engineering, and humanities literature (Brierley-Newell, 1995). While many have articulated core concepts in privacy, its very diversity gives rise to confusion in the vocabulary crafted to discuss privacy nuances. Different authors may use the same word to describe different concepts or phenomena, or the same author may use different words to describe the same concept/phenomenon without relating the words to one another. Disciplines have their own language, and thus interdisciplinary discussion of privacy is made complicated by obvious differences among the stereotypical conceptions of privacy in different domains. Lawyers stereotypically equate privacy with autonomy (being let alone). Psychologists stereotypically equate privacy with solitude (being apart from others). Technologists, economists, architects and others stereotypically equate privacy with confidentiality (keeping secrets).

The goal of this chapter is to unravel this confusion by describing a vocabulary of terms that permit unambiguous and holistic description of privacy in the context of video media space design and use. Collectively, this vocabulary creates a descriptive ‘theory’ about factors affection privacy and its perception. This vocabulary is grounded atop a broad base formed out of others’ theoretical descriptions of privacy, i.e., Altman (1975), Bellotti (1998), Palen & Dourish (2003), and Schwartz (1968). The vocabulary explanations below distil concepts explained in detail in our own prior work (Boyle, Edwards, & Greenberg 2000; Neustaedter & Greenberg 2003; Neustaedter 2003; Boyle 2005; Boyle, & Greenberg 2005; Neustaedter, Greenberg, & Boyle 2006), which in turn should be used as a source for further explication.

Tables 1 - 5 outline the vocabulary of terms that will be discussed throughout the chapter. Within the text below, terms are bolded and a reference to their location in the tables is included. For example, if the text reads **norms** (3.b.ii) then the vocabulary term, norms, can be found in Table 3 under item (b) and sub-item (ii).Our discussion of the vocabulary terms synthesizes the existing literature, presents new insights and organization, and directly relates the discussion to VMS design itself (at least as much as space allows).

We begin with an overview. Section 2 outlines the varying perspectives and approaches to understanding privacy in media space design. Section 3 builds on this work by outlining three control modalities for privacy in VMS—solitude, confidentiality, and autonomy—that form the core of our descriptive theory. The tables are central to our discussions, and should be read in their own right before starting. The tables by themselves should be considered a chart categorizing and classifying the various privacy vocabulary terms, while the text explicates the meanings of the words within it. While the tables are presented as a hierarchy, it is really a semantic web; thus our descriptions of terms often go across the categories and classification boundaries in Tables 1 - 5.

2 Perspectives on Privacy

“Private” is often defined as the opposite of “public:” public is to “being together” as private is to “being apart.” Brierley-Newell (1998) found this to be the most fundamental and broadly cross-cultural conceptualisation of privacy. Being apart is different from being alone though. For example, one can be with one’s lover and the two together are apart from a larger group. The part of one’s life lived apart from society was not highly valued in some ancient societies (Hixon, 1987) and strong emphasis was placed on social involvement. Palen & Dourish (2003) call this the **disclosure boundary tension** (4.d.vii): a tension between one wanting/needing/choosing/being private versus public. This tension carries over to VMS design. From an organisational perspective, the video media space is seen positively as it strives to increase the amount of ‘togetherness’ experienced by group members, even though the heightened collaboration and cooperative work may not be something desired by all individuals at all times.

2.1 Privacy as an Interpersonal Process

One perspective of privacy identified by Brierley-Newell is that human behaviours are part of a **privacy process** (4.b). Altman (1975) in particular sees it as a boundary-**regulation** (4.b.iii) process which facilitates the negotiation of access to the self. The **self** (3.a) broadly refers to the totality of a person: her/his body, thoughts and personality, and information about her/him. The negotiation occurs between the self and the **environment** (4.e): the physical environment and also the social environment i.e., the people immediately nearby and society at large.

Altman's privacy process is a **dialectic** (4.b.i). The actual level of privacy attained is decided through a process of negotiation between the self and the environment. This dialectic is **normative** (3.b.ii). Altman draws a sharp distinction between desired privacy and attained privacy. People's desired privacy is constrained by the environment to socially accepted (normal) levels. What constitutes a privacy **violation** (4.c) is defined against the same set of norms, some of which may be codified as laws while others are part of the culture's tacit knowledge. Individual factors are also important. Each person possesses his/her own set of privacy **preferences** (3.b.ii.2) or 'personal norms' that determine his/her initial desired privacy level and subsequently influence the privacy dialect. Also, group norms change in response to changes in group membership and so are influenced by individual preferences. This means that privacy regulation is **dynamic** (4.b.ii) and requires the **cooperation** (4.b.iv) of others. Making things even more complicated, there may be a number of norms that can apply in a given situation because one is typically involved in many groups simultaneously, or because of cross-cultural contact.

Altman's privacy process does not deny interactions between the self and the environment rather it regulates them. When one has too many interactions or, in other words, too little privacy, these interactions can be throttled. For example, a person turns off the media space to get away from others. When the connections with others have been cut so deeply that one has 'too much privacy' the privacy process can open access to the self so that a person gets the interactions he craves. For example, a person turns on the media space when he wants to chat with others. This process demands skill or, more likely, **power** (3.b.i.2) that not all persons share equally (Brierley-Newell, 1998) and power relationships become significant when addressing privacy problems in VMS design (Dourish, 1993).

2.2 Privacy as a Need, Right, and Freedom

People place great value upon privacy in our society. Privacy is often defined as a legal and moral right and as an inalienable freedom that no other person or institution may lawfully or morally unduly curtail. A privacy that is a right or freedom can be **violated** (4.c). Others' actions may deny one this right or impair one's exercise of it. Thus, it is a privacy violation when others' actions prevent one from obtaining the privacy he needs, he normally enjoys, and society deems that he ought to enjoy. Outcomes vary in **severity** (4.c.iv), which is a subjective measure of how 'bad' the harm due to the outcome is.

Privacy can be threatened without necessarily being violated. Privacy **threat** (4.c.v) and privacy **risk** (4.c.i) are used almost synonymously and seem to include the **possibility** (4.c.ii) of a violation, the **probability** (4.c.iii) that it will occur, and the severity of the harm it causes. Risk is quite inescapable: abstractly, if there is insufficient control to outright deny the possibility that a violation can occur, then there is some risk. Practically, however, opportunities for violation are held in check by **policing** (4.d.iii): providing punishments, taboos, social consequences such as **resentment** (5.b.iii), etc., to discourage others from doing things that violate one's privacy.

2.3 Privacy as a Balancing Act

Aside from hermits and the like, people balance the benefits accrued from social interactions against the risks to privacy, engaging and withdrawing from others to satisfy both the need to be 'apart' and the need to be 'together.' Even though there is risk, there may also be **reward** (4.d.v): benefits to having less privacy than may be possible. Thus, a **trade-off** between **risk and reward** (4.d.vi) exists.

People balance risk and reward in unmediated interactions but come up against problems when attempting to do so in mediated interactions. The technology itself, the ways it can be subverted, and the awkwardness of its interface may hinder their ability to port unmediated interaction skills to the virtual environment. For example, many video media space designs permit some form of **surreptitious surveillance** (2.c.iii.1), i.e., close monitoring or **analysis** (2.c.iii.2) of the environment—usually the presence and activities of others—without revealing much about oneself. This kind of surveillance can come about from seemingly innocent actions. Thus, video media space designs themselves foster **disparity** (5.c.ii) between risk and reward such that reward does not accrue accordingly with risk or, conversely, risk does rise with reward. This concept is illustrated in the subsequent chapter by Friedman et al. where they investigate privacy in public places. Surveillance is also brought up in Chapter 3.4 by Bill Buxton when the admin is concerned about her superiors watching her.

Reciprocity (4.e.vi) is a simple rule that states that if *A* can access *B* via channel *C*, then *B* can also access *A* via channel *C*. Reciprocity is often enforced over video media space channels as a technological means for re-balancing this risk/reward disparity (Root, 1988). Yet, reciprocity does not always hold for the physical environment, and sometimes breaking the reciprocity rule is beneficial. For example, it is possible to observe a person to deduce her/his **availability** (1.c.i.1)—willingness to engage in interaction—without disturbing her/him, such as by moving quietly and peeking around the corner of an open office doorway. Some VMS designs, such as the RAVE media, have explored privacy regulation in the absence of reciprocity but these design experiences underscore the need for multiple modalities of support for privacy in any one given system and across systems (Gaver et al, 1992).

2.4 Privacy Violations

A fundamental premise of much privacy research is that privacy is a thing that can be intentionally controlled (to a limited extent) by groups and individuals. This control is afforded by environmental constraints to interactivity. Technology confounds privacy control by lifting or changing these constraints (Palen & Dourish, 2003; Grudin, 2001) and affords new **degrees of temporal and spatial freedom for information access** (5.c.i) (Palen & Dourish, 2003). There is an implicit assumption that there are some times when some people—who may or may not be part of the VMS community—go out of their way to violate others' privacy. Thus, even though video media space users might never willingly violate their peers' privacy the system affords the potential for such **deliberate abuses** (5.b.vi*)*. Worse, media spaces are not adequately designed to safeguard against malicious use arising from unauthorised access. Thus, they afford the potential for undiagnosed abuse by outsiders. One example is surreptitious surveillance, which comes up in the Chapter 9 Friedman et al's discussion of privacy in public.

Undoubtedly, not all privacy violations are deliberate nor are all opportunities for deliberate privacy abuses capitalised upon. Accidental violations are known to happen from time to time. **Inadvertent privacy infractions** (5.b.i) are believed to occur because media space designs fit poorly with individual human and social factors thereby causing breakdowns in normal social practice (Bellotti, 1998). Specifically, privacy regulation is **situated action** (4.e.i) (Suchman, 1987). Environmental constraints for interactivity keep interactions situated in a temporally and spatially localised context. Technology changes these constraints, causing actions and interactions to be **desituated** and **decontextualised** (5.b.iv) (Grudin, 2001). That is, actions are seen out of their context, or the context is not communicated along with the action.

Related to this is the concept of **self-appropriation** (4.d.i): a regulatory process where people modify their behaviour and appearance according to social norms and expectations (Bellotti, 1998). Self-appropriation depends on cues for behaviour sense from the environment, such as **place** (3.b.ii.6) and the people in it. For example when a person is at work, she acts, dresses, and speaks to match others' expectations of professionalism. This will differ markedly from how she appropriates herself on the basketball court. As people move between contexts—the office, the bathroom, the hallway, the basketball court, the home—they modify their expectations for social behaviour (norms) and adapt their behaviour accordingly. The impoverished nature of a video media space means that people often do not appropriate themselves correctly for viewing by distant colleagues. **Disembodiment** (5.b.iv)—where a user becomes cut off from the (multiple) contexts of those people viewing him—confounds self-appropriation and leads to inadvertent privacy violations (Bellotti, 1998).

Privacy violations can be **aesthetic** (3.a.iv.1)—affecting appearances and impressions— or **strategic** (3.a.iv.2)—affecting the execution of plans (Samarajiva, 1997). In social environments, aesthetic privacy violations can have consequences of a strategic nature. Humans, as social creatures, fear and resent both kinds of violations. Non-users are often so suspicious of the media space that they go out of their way to sabotage the system (Jancke et al, 2001). Even users themselves are often wary about the system's handling of their privacy (Tang et al, 1994). Thus, in addition to specific deliberate or inadvertent privacy threats, prior analysis of video media space privacy indicates that **apprehension** (5.b.ii) itself is a significant problem. Specifically, participants are apprehensive about making bad **impressions** (3.a.i.4) in the media space and the aesthetic or strategic consequences of them.

2.5 Privacy Control in Media Spaces

One way to solve deliberate privacy abuses is with **access control** (5.a.iv), which puts into place computer security and cryptographic measures to deny unauthorised individuals access to sensitive information (Smith et al, 1995). While access control is common on virtually all computers, those wishing to restrict access have faced a constant and unrelenting battle with those wishing to crack systems. Another way to solve deliberate privacy abuses is to simply remove sensitive information from the media space so there is nothing of worth for others to access and to reduce the harm that may result if access control measures are defeated. We call this technique **content control** (5.a.v). It is hard to put this technique into practice in a VMS because the purpose of a media space is to reveal (Gaver et al, 1992). There is a fundamental trade-off between privacy and the **utility** (5.c.iii.3) of VMS for awareness: for one person in the media space to have richer awareness, others must have necessarily less privacy (Hudson & Smith, 1996).

Figure 1 shows several techniques for preserving privacy in video media spaces based on content control. **Distortion filters** (5.a.v.1) such as the blur filter in Figure 1 mask sensitive details in video while still providing a low-fidelity overview useful for awareness (Zhao & Stasko, 1998; Boyle, Edwards & Greenberg, 2000). The technique itself is a kind of **edit** (2.c.i.3) operation that occurs after **capture** (2.c.i.1). Distortion filtration operates solely on the **visual information channel** (2.a.i.2). The information is obtained directly from **sampling** (2.a.ii.1) the visual field, rather than being **interpolated** (2.a.ii.2), **aggregated** (2.a.ii.3), or **inferred** (2.a.ii.4) from multiple other context sources. The distorted video image contains some **personally identifying information** (2.a.iii.2), namely people's faces, but mostly contains information that we call **information about the self** (2.a.iii.1): the **actions** (2.a.iii.7) and **activities** (2.a.iii.3), **whereabouts** (2.a.iii.4), and **encounters** (2.a.iii.5) of a person that may or may not be known to or identified by an observer. **Publication filters** (5.a.v.2) such as the background subtraction filter in Figure 1 are similar to distortion filters. They work by removing details from the visual channel that are considered unimportant for awareness information (Coutaz et al, 1998; Junestrand, Keijer & Tollmar, 2001). Finally, potentially privacy-threatening details can be also abstracted away from the video altogether such as in instant messenger status icons and in the eigenspace filter in the figure (Crowley et al, 2000).

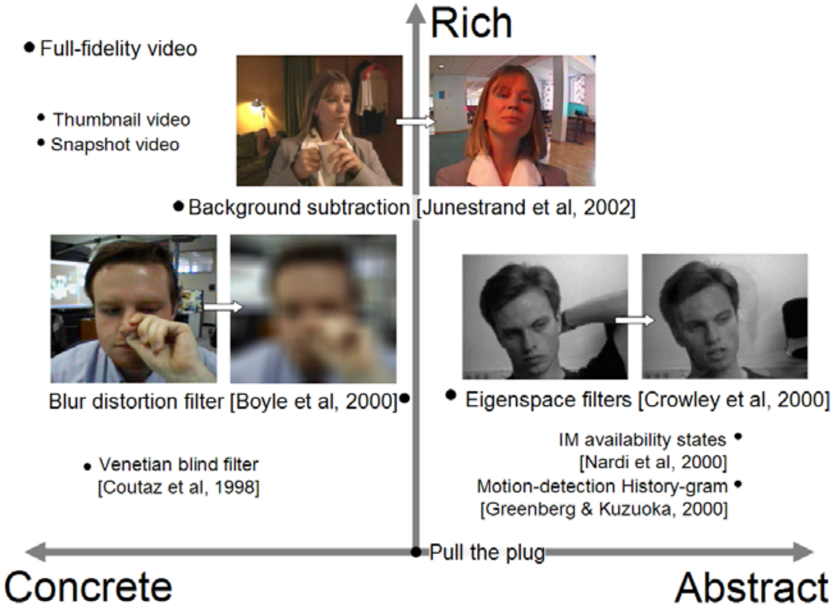
Rich
Full-fidelity video
Thumbnail video
Snapshot video
Background subtraction [Junestrand et al, 2002]
Blur distortion filter [Boyle et al, 2000]
Eigenspace filters [Crowley et al, 2000]
IM availability states [Nardi et al, 2000]
Motion-detection History-gram [Greenberg & Kuzuoka, 2000]
Venetian blind filter [Coutaz et al, 1998]
Pull the plug
Concrete
Abstract

Fig. 1 A design space showing some previously explored techniques for preserving privacy in video media spaces.

The above approaches involve control over what information is in the media space and who gets to see it. It is hard to design a video media space that provides fine-grained control in a lightweight manner, yet both are vital to preserving privacy (Bellotti, 1998). **Fine-grained control** (5.c.v.1) can be adjusted on a person-by-person, instance-by-instance basis. **Lightweight control** (5.c.iv.3) needs little **cognitive** (5.c.iv.1) or **physical** (5.c.iv.2) effort. In the physical environment, strategies for controlling information access are both lightweight and fine-grained. Yet there are few fine-grained yet lightweight strategies for controlling a video media space. Unplugging the camera is a lightweight and undeniably effective means for blocking access to all, but it is not very fine-grained—the video channel is blocked for all recipients.

Control user interfaces must also be **believable** (5.c.iii.1): be readily understood and effect meaningful change in a predictable manner. Control must also be easily interpreted by others. **Dissociation** (5.b.iv), where one's actions become logically separated from one's identity, makes it very difficult for VMS participants to determine who is accessing information about them even though they may be able to tell that it is being accessed (Bellotti, 1998). Dissociation makes deliberate privacy abuses possible because information can be accessed in an unchecked, untraceable, and anonymous manner (Langheinrich, 2001). People have poor strategies for dealing with dissociation because it rarely occurs in the physical environment: one's body, as it is performing an action or gaining access, communicates a wealth of identifying information, coupling action to identity.

2.6 Privacy Feedback in Media Spaces

The design of **feedback** (4.e.x.1) channels to support self-appropriation is fraught with technical factors that permit inadvertent privacy violations. It is hard to balance VMS feedback **salience** (1.c.ii.2) and **distraction** (1.c.ii) (Gaver et al, 1992; Hudson & Smith, 1996; Bellotti, 1998). If feedback cues are not saliently presented they will go unnoticed, fostering disembodiment and poor self-appropriation. If feedback cues are too distracting, such as lacking **relevance** (1.c.ii.1), there is the risk that the VMS user will either disable the feedback channel or disable the VMS altogether. **Feed-through** (4.e.x.2)—the transmission of cues signalling an action as it is in progress—is related to feedback and is similarly problematic.

It is hard to design VMS feedback cues for self-appropriation that integrate well with social protocol for conversation initiation. In the physical environment, feedback cues are given **socially natural** (5.c.iii.2) forms, placements, and meanings. For example, a person in his office can hear, emanating from the corridor, the footsteps of a colleague approaching him to strike up a conversation. This audible cue signals the onset of interactivity (who, when, and where) and there is a rich, socially-based (and often unconscious) protocol for initiating conversations built around this doorway approach. Providing a media space user interface to support this protocol is full of subtle problems.

Bellotti presents a framework for analysing deliberate and inadvertent privacy problems in systems and evaluating solutions (Bellotti, 1998). Her framework consists of topic areas for formulating questions about the feedback and control a system affords over information in it and topic areas for evaluating the feedback and control user interface. Bellotti's framework includes **intention** (2.c.ii) for access and minimal needed disclosure as feedback cues that are important to evaluating privacy options. In unmediated settings, intention may be revealed implicitly as a consequence of an attempt to access (prior to access is made) or through explicit (e.g., verbal) communication of it. In either case, the communication process is kept extremely lightweight. It is not lightweight in media spaces. Disembodiment and disassociation confound the implicit signalling of intentionality before access is made. Even if there are audio or text channels, getting everyone into a state where they can use them is not lightweight. Beyond cumbersome user interfaces, networking delays during the initiation of conversation denies quick and graceful transition into it (Tang et al, 1994).

3 Privacy as Control Modalities

Many discussions of media spaces attribute privacy problems to inadequacies in control and its exercise (Bellotti, 1998, Grudin, 2001, Palen & Dourish, 2003). For this reason, our descriptive theory of privacy identifies three control modalities by which people control the self-environment boundary (Altman, 1975). These modalities are based on the elements of privacy outlined by Gavison (1980). The control modalities we identify are:

- **Solitude**: control over one's interpersonal interactions, specifically one's attention for interaction (1).
- **Confidentiality**: control over other's access to information about oneself, specifically the fidelity of such accesses (2).
- **Autonomy**: control over the observable manifestations of the self, such as action, appearance, impression and identity (3).

All three modalities of control are negotiated concurrently. Behaviours used to exert one modality of control also have strengthening and weakening implications for the other two. Moreover, 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.

A similar approach has been taken up by Palen & Dourish (2003). In their framework they identify three boundaries which are congruent to but not direct parallels of the three modalities of privacy control we describe here. The **disclosure boundary** (4.a.i) is regulated mostly by confidentiality, but also by solitude. The **identity boundary** (4.a.iv) is regulated by autonomy. The **temporal boundary** (4.a.ii) spans both identity and disclosure and is regulated by the norms and preferences that are part of solitude, confidentiality and autonomy.

In the next three sections we delve deeply into each of the three modalities of control—solitude, confidentiality and autonomy—to complete the construction of an integrated vocabulary for privacy.

4 Solitude

Solitude controls help a person 'be apart' from others and are involved in many behaviours that are vital to human development, e.g., self-evaluation and ego development (Altman, 1975). Being apart is different from being alone: for example, two lovers can find solitude in each other's company, even in a crowded restaurant. 'Togetherness' is thus a continuum of states, and the extremes present failure conditions that yield negative behavioural, psychological, and physiological responses. For example, **crowding** (1.a.i.1) results when others are granted too much access to the self. **Isolation** (1.a.i.1) results when one cannot interact with others to the degree they wish. Both conditions indicate failures in solitude control. Westin (1967) introduces four states along a spectrum of social interactions arising from typical exercise of solitude. These include:

- total isolation (Westin calls this 'solitude');
- **intimacy** (1.b.i.1)—the state in which a small group (e.g., lovers) isolate themselves from others;
- **anonymity** (1.b.i.1)—the state in which one is physically co-present with others and yet not expected to be recognised by them; thus being free from interactions with them (e.g., 'lost in a crowd'); and,
- **reserve** (1.b.i.1 and 4.d.ix)—the state in which we can ignore the presence of others who are nearby.

We also generalize solitude to include control over where one directs one's **attention** (1.a.ii)—ranging from one's **focus** to being in the **periphery** (1.a.ii.1)—and how one controls **distraction** (1.c.ii). Most video media spaces require that users expend extra effort to attend to awareness information by presenting it in ways that potentially distract or disrupt people. Thus, media spaces confound solitude, and presence and **availability** (1.c.i) are regulated by solitude. This also relates to problems of 'camera shyness' (Lee et al, 1997) where the heightened self-awareness that people are monitoring one's availability can lead to discomfort (Duval & Wicklund, 1972).

4.1 Verbal and Para-Verbal Solitude Controls

A variety of individual and social behaviours are used to regulate solitude. Verbal and para-verbal mechanisms for controlling solitude usually involve signalling availability, e.g., verbally telling another you wish to be left alone or hanging a 'do not disturb' sign outside a hotel door. Desires can be signalled in both the content (the meaning of the words spoken) and the structure (pitch, duration, volume etc. of voice) of speech (Altman & Chemers, 1980). Para-verbal means for signalling one's desired solitude include a posture or facial expressions and explicit gestures to beckon or dismiss others. While these mechanisms are very lightweight in face to face settings, they are easily impaired by limitations of VMS technology. For example, low-quality video (i.e., low resolution, low frame rate, many visible artefacts of compression) mask subtle para-verbal cues for communicating availability. Because such desires must instead be communicated with speech, video media spaces can make the process of signalling solitude desires more explicit and heavyweight. These changes alter social interpretation of the expressed desires.

4.2 Affordances of Space for Solitude

To regulate solitude, one can also go someplace to be alone. These places of **refuge** (1.b.ii.1 and 4.e.viii) permit one to 'get away' from the stresses incurred through interactions with others by utilizing **spatial boundaries** (4.a.iii). Yet VMS design complicates refuge-seeking. Although places of refuge from the media space are typically nearby—it is prohibitively expensive to put cameras in every room and so the media space is usually present in only a few locations (e.g., in a person's personal office). Awkwardly, the office is where most will retreat to find refuge. A place of refuge can also be created by 'pulling the plug' on the video media space (Neustaedter and Greenberg, 2003). Unfortunately, this disconnected mode of operation is often misinterpreted in many media space implementations as an exceptional error case to which little developer attention is given. Consequently, most hardware and software infrastructures make reconnection so complicated that users are disinclined to 'pull the plug.'

Conversely, when one craves social stimulation, one can go to places where others are. Place partially determines **accessibility** (1.c.i.2), i.e., the effort people must expend to engage others for interaction (Harrison & Dourish, 1996). Architectural spaces can often be reconfigured to raise or lower their permeability to light, matter, and sound. In changing these attributes, people control the affordance of space for interactivity. For example, an office door can be closed to reduce visual and auditory distractions from the corridor and serve as a physical barrier to others' entry. Doors permit fine-grained control because they can be fully closed, slightly ajar, or wide open. Indeed, this becomes a social cue indicating one's solitude desires. In contrast, video media spaces generally provide only one modality for interactivity (an audio/video channel) and offer few ways to configure this channel to signal the desired level of engagement.

People can also capitalise upon the ambiguity inherent in some architectural changes to regulate solitude. For example, a closed door ambiguously symbolises both absence as well as a wish to be left undisturbed (Root, 1988). People also capitalise on **ambiguity** (2.b.iii.2) when it is possible in computer-mediated environments. For example, Nardi et al (2000) report that people use the inaccuracies of IM presence indicators as a form of **plausible deniability** (2.b.iii.1) where they ignore requests for conversation from people because they know that the other person will be uncertain if they are really there.

4.3 Personal Space

Space and social behaviour interoperate with respect to solitude. **Personal space** (3.a.i.5) refers to an invisible boundary in space around a person, separating him from others. The boundary's shape and size varies from moment to moment as part of the privacy dialectic. Although the boundary's characteristics are never made explicit, people show definite behavioural and physiological responses when others physically enter their personal space. **Territory** (3.a.iii.1) is similar, but usually implies a recognisably fixed spatial or psychological location, even if it is defined relative to its owner. Territories are important for the regulation of workspace artefacts and confidentiality and will be discussed later.

Personal space regulates solitude by reducing sensory stimulation due to the presence of or interactions with others. This, in turn, affects attention. At each distance, different sensory capabilities afford different modes for interaction. Hall describes four interpersonal zones, each with differing modalities for social interaction; these are given in Table 6 (Hall, 1966). Because of this relationship between distance and interaction, distance itself becomes imbued with social meaning (Altman, 1975). For example, consider when one person sits down at the same table as another. If the newcomer sits diagonally across the table and out of direct eye contact, he sends a solitude-related message that differs markedly from when he chooses to sit directly across the person and in easy eye contact.

Distance	Modality	Interaction Capabilities
Public Distance (>5m)	Gross Vision	Gross assessments of posture and large gestures; facial expressions and gaze not visible
Social Distance (<4m)	Hearing	Speech content and structure
Personal Distance (<2m)	Detailed Vision	Posture; gestures; gaze; facial expressions involving eyes and mouth (e.g., wink, smile)
Interpersonal Zone (<0.5m)	Touch and Smell	Exchange, inspect, and manipulate artifacts; physical contact (e.g., handshake, hug); perfume

Table 6 Interpersonal distances and the interactions supported at each (Hall, 1966).

Personal space, as a tool for solitude regulation, depends on having a range of **interpersonal distances** (1.a.i) at which people may space themselves. These distances define modalities for interaction that differ in both affordances for interaction and the attention or engagement needed to sustain such interactions. These distances are thus imbued with social meanings. Typically, in a video media space the camera position and display size dictates the visual distance between people; these are sometimes arbitrary and do not represent the desired social distance. For example, seeing a tightly cropped face shot on a large video monitor places someone visually close, but the mannerisms exhibited by that person may reflect actions of someone who is in fact quite far away.

The concept of interpersonal distance in a VMS can be even further generalised to include engagement and connectivity. In a typical VMS, only two or three such distances are offered: full interconnectivity; connected to just one other person; and, disconnected from everyone. The limited choices for connectivity make the media space a crude tool for the selective expression of social interest for interactivity. Moreover, in physically co-located settings, adjusting distances is very lightweight and can be continuously adapted by just moving around. In contrast, media spaces offer highly discrete choices selected using heavyweight GUIs and limit degrees of freedom, e.g., it is awkward to reposition the VMS camera because of limited cable lengths, lighting, shelf space, and similar factors.

5 Confidentiality

Confidentiality is the control of access to information about oneself, e.g., informal awareness cues, intentions, vital statistics, thoughts and feelings, medical history, criminal record. Thus, confidentiality is about controlling **aural** (2.a.i.1), **visual** (2.a.i.2), **numeric** (2.a.i.3), and even **textual** (2.a.i.4) information. Controlling access is as much granting access as it is restricting it. Secrecy is similar to confidentiality but narrower because secrecy emphasises that the information is concealed from certain people. Secrecy modulates the communication of information to others, but this is only one aspect of confidentiality. Palen & Dourish (2003) use the term disclosure to describe deliberate control over what information is communicated, to whom, when, and how.

Confidentiality and solitude are of course related. Confidentiality directly regulates the outward flow of information and thereby indirectly others' attention, whereas solitude directly regulates one's own attention by indirectly regulating the inward flow of information from others. As noted earlier, there is a fundamental tension between confidentiality and the goal of the video media space to reveal informal awareness cues (the disclosure boundary tension described by Palen & Dourish). Hence, there is tension regarding confidentiality in the design of a video media space. Confidentiality and autonomy are related as information yields power to affect livelihood (e.g., coercion, competitive advantage), personal safety or autonomy (e.g., interference or intervention).

Sensitivity (2.b.i.1) is a property of a piece of information that can be defined as a perception of how important it is to maintain control over access to it (Adams, 2000). Others' impressions of a person are predicated upon their knowledge of her, and so confidentiality is part of impression management (Goffman, 1959). The harms that could arise from breeches of confidentiality include embarrassment, damage to ego and identity, loss of others' esteem, and possibly impairment of livelihood. Video media spaces can, of course, easily reveal sensitive information when they unintentionally capture and transmit a person's image that, for example, shows that person in a socially unacceptable act.

5.1 Computers and Confidentiality

Increasingly, computers are being used to store or transmit confidential information and **computer security** (5.a.i) holistically addresses many aspects of confidentiality. **Authorisation** (5.a.iv.2) is control not only over access, but also use, i.e., a person's intention for using the system or the information it provides, or outcomes of access. **Data integrity** (5.a.vi.1) concerns ensuring that persisted information about oneself is not modified or transmitted information is not modified en-route. Both of these are obviously part of confidentiality. **Process integrity** (5.a.vi.2), availability, responsiveness, and reliability concern ensuring that computers perform their intended function when requested correctly and completely in an expected amount of time with no undesired side-effects. Process integrity is an important component of confidentiality because, as stated in the introduction to this section, confidentiality includes ensuring a person has all the access he/she has been granted. **Cryptographic methods** (5.a.ii) are used to provide access control and verify the identity of the receiver or sender of information and check the integrity of the message (e.g., with digital signatures).

5.2 Fidelity

Fidelity (2.b.ii) is one aspect of confidentiality that has been studied in detail as it relates to VMS design. Fidelity is a perception of how faithfully a piece of information represents some truth. It includes both **precision** (2.b.ii.1)—how detailed the information is perceived— and **accuracy** (2.b.ii.2)—the confidence or certainty one places in the information, or the error in its perception. The same essential truth or description of circumstance may be perceived at a variety of fidelities. Information about oneself—the object of confidentiality—may be known by different individuals at different fidelities. The perceived fidelity of information is also not static. It is influenced by the **trust** (3.b.i.5) one places in the sender and the number of recipients. We also consider that information has properties such as **persistency** (2.b.i.2) and **transitivity** (2.b.i.3) that are relevant to confidentiality. Information may change when it is transmitted between people, such as through oral or written statements or when it is permanently recorded. Hence, confidentiality also involves the regulation of the fidelity of information that third parties transmit about us.

Within VMS design, confidentiality includes control over fidelity. Confidentiality is breeched when a person is unable to control the fidelity at which others are able to access her/his information. Video media spaces have several dimensions for video fidelity, e.g., field of view, resolution, frame rate, codec quality, latency, jitter, etc. Technology places an upper bound on most of these parameters, and these bounds are usually much lower than in face to face situations. For example, although a person can move his head or body to very easily change his field of view to encompass virtually any area around that person, the field of view in a video media space is typically fixed because the cameras lack pan/tilt/zoom capabilities.

Despite these upper bounds, video is nonetheless a high-fidelity medium for informal awareness and casual interactions. This is both part of the appeal of video and a source of confidentiality problems. Undoubtedly, video offers more fidelity than is genuinely needed in many scenarios, even between intimate collaborators. Consequently, many video media space designs try to preserve confidentiality by discarding fidelity. This typically involves using techniques that mask the video with distortion filters such as a blur filter (Boyle et al, 2000). The premise is that appropriate masking can find a balance by providing just enough awareness information to be useful, while not too much to violate confidentiality. These techniques presume that sensitive information lays mostly in image details and so low fidelity overviews of the video pose less risk (Hudson & Smith, 1996). Studies have shown, however, that the effectiveness of such techniques is limited when risky situations may be captured by the VMS (Neustaedter 2003; Neustaedter and Greenberg, 2003; Neustaedter et al 2006).

5.3 Direct Controls

Mechanisms for regulating confidentiality overlap greatly with those for solitude, emphasising their synergistic relationship. The principle means for confidentiality control involve keeping our bodies, possessions, and thoughts accessible to some but inaccessible to others. We consider possessions because things like diaries, driver's licenses and even automobiles reveal a great deal of sensitive information about a person and are used to mark status and individuality (Schwartz, 1968). Territoriality and personal space use distance to afford fine-grained control over others' access to our bodies and our things. Similar control is available over speech: a person directs his voice and modulates its volume so as to whisper into the ear of someone nearby without allowing others to hear what is said. Private vocabularies can be used to talk openly among others yet obscure what is being said: e.g., pig latin among children and hand signals in baseball.

Architecture also plays a vital role in the preservation of confidentiality (minimising leaks out) as well as the preservation of solitude (minimising leaks in). Walls reduce access via visual and auditory channels. Walls may also be fortified with sound-proofing materials to preserve aural confidentiality as well as solitude. Window blinds may be raised or lowered and doors closed or open to modulate visual confidentiality. Video media spaces afford similar opportunities for regulating confidentiality, e.g., turning down microphone volume so as not to be overheard, encoding information with cryptographic methods so others cannot eavesdrop, or using a filtration technique (Boyle et al, 2001).

5.4 Indirect Controls

People explicitly state (verbally or para-verbally) their confidentiality desires and perceptions on information sensitivity. For example, one person can tell another to "Keep this secret, okay?" Telling a person that it is important to keep a piece of information secret does not prevent that person from revealing it to others. Yet, people can choose to—and sometimes do—keep others' secrets. People can intuit others' sensitivity perceptions and from these infer self-imposed limits to behaviour. While people can keep secrets or assess sensitivity, a particular individual may not keep a secret well, or may ultimately choose not to respect the apparent sensitivity.

Information about others, including confidentiality preferences, are usually revealed over time as one builds and maintains **relationships** (2.a.iii.8) with others. Palen & Dourish (2003) introduce the notion of **genres of disclosure** (4.d.ii) to capture not only institutional (socially constructed) expectations regarding confidentiality but also situational ones that change with the temporal boundary. That is, genres of disclosure are loosely defined patterns of interactions that evolve over time. Because genres of disclosure are loosely defined between people, it is possible to feel that one's privacy has been violated through others' **misappropriation** (2.c.ii.2 and 5.b.vi.1) or **misuse** (2.c.ii.3 and 5.b.vi.2) of confidential information and not just inappropriate disclosure.

VMS may change the rules of engagement however. For example, a VMS might permanently **archive** (2.c.i.2) video/audio exchanges for later replay, rendering requests to keep information confidential meaningless. Verbally telling those people present to keep matters confidential does not preclude others from listening in later. By the same token, people willingly and unwittingly spread **misinformation** (2.b.ii.3)—unintentionally inaccurate information—and **disinformation** (2.b.ii.4 and 4.d.viii)—intentionally inaccurate information designed to obscure the truth, i.e., lies. Given this, it is important to incorporate into the VMS design various awareness and interaction channels that can be used to diagnose, police, and **reprimand** (4.d.iv) wilful and damaging violations. Similarly, VMS designs should be **accountable** (2.c.ii.1) by letting users know how their sensitive information is being handled within the system.

6 Autonomy

Collectively, the freedom to choose how one acts and interacts in the world (freedom of will, also liberty) and the power to act in such a way are taken as the third modality of privacy control: autonomy. In law, **personal liberty** (4.e.vii) is often used synonymously with autonomy. Self-appropriation, described earlier, and autonomy point to the same basic control—control over one's own behaviour—yet, autonomy incorporates behaviours that facilitate self-definition and identity. Privacy problems in video media spaces can often be blamed on systems' poor support for managing behaviour, identity and impressions. Thus, an understanding of autonomy—which regulates these things—is needed to design a privacy-preserving VMS.

6.1 Preserving and Constraining Autonomy

Autonomy is like the ‘muscle’ of privacy in that it must be routinely exercised or it will atrophy. The simplest mechanism for preserving autonomy is to try to do as one wishes. One can communicate to others how important it is that she be allowed to do precisely as she wishes. Such signalling may be **explicit** (4.d.x.2) in the content of speech or **implicit** (4.d.x.1) in the structure of spoken language, facial expressions, and posture. Informal awareness cues for availability simultaneously reveal one’s autonomy desires.

Autonomy can be impaired when technology robs media space users of the opportunity to choose when and how they participate in the media space community. While there are cases in which media space participation is effectively mandated by an organisation’s culture, in such cases the social fabric of the organisation has evolved through an extended period of use (Harper, 1996). Introducing video into home offices also engenders several different kinds of privacy fears, one of which is related to loss of autonomy. One of the advantages of working from home is the ability to set one’s own schedule. Home workers often work at irregular times outside the typical “9 to 5” hours to better accommodate the demands of family life they hope to balance by working at home in the first place. A video media space that connects home and corporate offices blurs the clear separation between one’s presence at home and one’s presence at work. This could introduce social pressure to schedule one’s activities at home to fit the work context, effectively robbing them of the opportunity to decide when they work.

Exercising autonomy does not imply that one “always gets one’s way.” Although the sanctity of autonomy is enshrined in law—people are granted the rights and freedoms needed to enjoy life, each according to her/his own will—both autonomy and our legal entitlement to it take part in a dialectic based on group norms. Each may do as he/she wishes, so long as her/his actions conform to group **expectations** (3.b.ii.1). Indeed, as part of the normal regulation of autonomy, one routinely adjusts one’s behaviour so that one may live cordially among others. This involves acting in a manner that is **socially acceptable** (3.b.ii.3), which may entail **conforming** (3.b.ii.4) to group norms. This is essentially self-appropriation. Thus, autonomy is generally constrained rather than compromised by group norms. Yet, if group norms change faster than people can adapt, or insufficient feedback about the presence and activities of others is offered to support self-appropriation, autonomy can be compromised.

Beyond self-imposed limits to autonomy, others may directly constrain it. For example, institutionalised people often incur great losses in autonomy (Altman, 1975). Parents often restrict the autonomy of their young children to keep them safe and to socialise them (teach them how to behave properly in society). Constraints to autonomy are the primary means for punishing bad behaviour: adults who commit crimes are incarcerated and children who disobey their parents are grounded. These observations have implications for VMS design. Fundamentally, the single user interface to a social technology like video media spaces eliminates social governance of its use.

6.2 Autonomy-Confidentiality-Solitude Symbiosis

The second way in which autonomy is like the muscle of privacy regulation is that it provides people with the power to enact their privacy **choices** (4.e.v), i.e., to control information access and direct attention for interactions. Solitude and confidentiality intrinsically depend on autonomy in a readily understood way. Yet, the converse is also true: one cannot have autonomy without solitude and confidentiality. Solitude is needed for self-reflection and the formulation of future plans (Altman, 1975). Solitude also affords a person with confidentiality needed to perform socially unacceptable acts. Confidentiality is also needed to preserve autonomy when others can use privileged information to thwart one's short- and long-term plans. Because of the symbiotic relationship between solitude, confidentiality and autonomy, when a VMS design impairs the regulation of one kind of control, the other two may also be negatively affected. For example, when cameras are ubiquitously embedded into every corner of our physical space, their pervasiveness makes it difficult for people to find opportunities to be apart from others (i.e., regulate solitude) and thus limits choices for autonomy where they cannot do some desired behaviours because they are being watched.

Some important autonomy-related terms can be borrowed from Goffman's (1965) framework for self-presentation. People are actors who have **fronts** (3.a.i) which serve as conduits for the social expression of self and team identities. A front is manifested in actions, **utterances** (2.a.iii.6) and interactions as well as various verbal and non-verbal **signifiers** (3.a.iii): social setting such as location, scenery, **props** (3.a.iii.2); **appearance** (3.a.i.3) such as **costumes** (3.a.iii.3) and props, posture, expressions, gestures; and, manners. These signifiers have social meanings which contribute to the front. As such, fronts can become institutionalised and the audiences' expectations of a front become part of the front itself. Fronts are carefully constructed and maintained (for example, by confidentiality) to ensure homogeneity between performances. The **back** (3.a.ii) is a secondary presentation of the self to only the team (for team fronts) or the individual her/himself. Here, **deviance** (3.a.ii.2 and 3.b.ii.5) occurs and the self is maintained. If left unchecked, there is the possibility that unconscious back-stage performances such as **fantasy** (1.b.ii.2) can be made into lapses in desired self-appropriation in the front.

6.3 Identity

Autonomy also includes control over **identity** (3.a.i.1) and its expression, e.g., a person's likeness (visual physical appearance and mannerisms, and the sound of one's voice) and names (e.g., signature or seal). National identity cards, passports, driver's license, credit cards, and so forth are tangible artefacts revealing identity. These exist separately from a person's body and may be held in possession or reproduced by others. Electronic equivalents include email addresses, personal web pages, and network IDs. These make up part of one's **digital persona** (3.a.i.2) (Clarke, 1994). While there are legal safeguards to discourage others from mishandling one's conventional identity, such as civil penalties for libel or unauthorised use of one's identity to promote a product or service, these are still sadly lacking in the electronic medium. With no recourse to reprimand violators, computer system users must turn to privacy-enhancing technologies to protect their online identities, usually by preserving the confidentiality of one's digital persona (Burkert, 1998).

Identity is highly relevant to VMS design. Dissociation relates to identity because the virtual **embodiments** (4.e.ix) of people—which signal presence and afford means to interact with others and access information about them—do not, unlike our corporeal bodies, reveal identity. This is despite a range of possible embodiments offering varying degrees of information from **rich to impoverished** (4.e.ix.1). Computer security also relates. **Impersonation** (5.b.vi.4) is the act of assuming the identity of another, usually without authority. **Identity theft** (5.b.vi.3) is a form of impersonation that usually involves theft of documents used to **authenticate** (5.a.iv.1) (confirm the identity of) an individual. Confidentiality guards against this type of crime, but vigilance is required to keep identifying information and authenticating documents out of the hands of malicious individuals. Just as reserve promotes confidentiality, minimising the amount of identifying material that exists physically separate from an individual preserves her/his control over her/his own identity. Oddly enough, certain privacy-preserving techniques used in video media spaces can create situations that confuse identity. For example, distortion filters that greatly blur an image, or substitute actors in the video with stock images can make one person unintentionally appear as another (Crowley et al, 2000).

6.4 Pseudonymity

A person is typically involved in a number of intersecting and disjoint social worlds. **Pseuodnyms** (5.a.iii) are alternate identities which one creates and uses for interactions within each environment. Often, each identity is used in a distinct social world and little is revealed that relates one identity to the others. Transportation and telecommunication technologies facilitate pseudonymity by allowing social circles to extend across large geographic ranges and population bases, decreasing the likelihood that a person who is part of one social world is also part of or communicates with members of another. Also, some telecommunication technologies permit anonymity by allowing one's interactions with the environment to proceed in a way that limits the reveal of identifying information. Video media spaces are at odds with pseudonymity because much identifying information is communicated in the video image of one's face and body. While video manipulation techniques could conceivably replace a person's real visage with an artificial one, such algorithms are tricky to implement in practice, require considerable setup for creating replacement images for multiple identities, and likely reduce the value of the video channel for expressive communication.

6.5 Role Conflict

People often assume different **roles** (3.b.i.1) as they move between social worlds. A single person may have the role of a stern leader when working with underlings, a supplicant when working with her boss, a parent when with her children, a lover when with her mate, and a slob when alone at home. This implies possible **status divisions** (3.b.i.4) and can also create certain role **obligations** (3.b.i.3). **Role conflict** (5.b.v) (Adler & Adler, 1991) can result when previously non-overlapping social worlds collide and one is forced to assume two previously distinct roles simultaneously, exposing each to people whom one would rather not. The classical example of role conflict in the non-mediated environment is when parents go to visit their children at their college dormitory: the children must simultaneously play the role of 'children' in the eyes of their parents and 'adults' in the eyes of their peers.

Role conflict can be a major problem in video media spaces. The purpose of the media space is to connect physically distributed people, but its users will likely inhabit quite different physical contexts. By virtue of connecting two physically disjoint spaces—each embodying their own, possibly different sets of privacy norms—the media space creates opportunities for role conflict akin to problems with self-appropriation. Moreover, there is an analogue of role conflict for privacy norms: decontextualisation confuses which norms apply in a given circumstance (Palen & Dourish, 2003). These problems are particularly evident when the VMS connects both home and corporate offices. The home worker must simultaneously play the role of an office worker (because he is connected to the remote office site), a disciplinarian parent and intimate partner (when children or mates enter the home office) and a relaxed home inhabitant (when he is alone at home and forgets he is connected). Role conflict fosters opportunities for inadvertent privacy violations and contributes to the apprehension participants feel towards the media space.

7 Conclusion

This chapter has described a comprehensive vocabulary of privacy – a descriptive theory - that permits unambiguous description of privacy-related phenomena and issues connected with the design of video media spaces. This includes the discussion of various perspectives on privacy as it relates to video media space design, as well as three control modalities—solitude, confidentiality, and autonomy—used by people to regulate privacy in their environment.

The chapter does not explain how to apply this vocabulary. One approach is to systematically analyze video media space designs using our vocabulary and its discussion, a process described in detail by Boyle (2005). To summarize, designers and practitioners can analyze VMS designs using vocabulary terms from one or more of the sections reflected in Tables 1 - 5. They first select their focus in the table, and then systematically describe each aspect of their system in an unambiguous manner using the vocabulary terms from the descriptive theory. Subtle omissions or discrepancies between privacy as conceived in the descriptive theory versus privacy as embodied in the object of analysis highlight areas for future iteration on the design. It is not a checklist, as there could be good reasons for not attending to some of the phenomena implied by a particular vocabulary term. However, each term reminds the analyst about whether they have considered that phenomenon. Overall, this process should allow designers and practitioners to understand the merits and demerits of the design and any privacy safeguards found within it. This understanding can in turn indicate directions for further iterative or exploratory design. Boyle (2005) further applies this vocabulary to compare various privacy theories for completeness.

Naturally, there are limits to the work we have presented. It is not generative, i.e., it does not lead directly to design ideas, their implementation, or their evaluation. Rather, as a descriptive theory our work informs the *analysis* of video media space systems within their real world context. In particular, it is capable of revealing assumptions hidden in the design, or the implementation, or the evaluation (Boyle 2005).

Although there has been a considerable corpus of work relating privacy problems to the design of social technologies, there is tremendous work yet to be done. In particular, we still need to advance the state of our understanding from individual words that describe privacy, to axioms that explain what ‘privacy-preserving’ means, to models that will drive the design and verification of privacy supporting social technologies. It is likely that each term in our vocabulary could generate a research investigation in its own right! Our work is a first step in this direction.

References

1 Adams A (2000) Multimedia Information Changes the Whole Privacy Ballgame, in *Procceedings of Computers, Freedom, and Privacy 2000: Challenging the Assumptions*. (Toronto, Ontario, Canada), ACM Press 25-32

2 Adler P, & Adler P (1991) *Backboards and Blackboards*. Columbia University Press, New York, NY

3 Altman I (1975) *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Wadsworth Publishing Company

4 Altman I, & Chemers M (1980) *Culture and Environment*. Wadsworth Publishing Company, Stanford, CT

5 Bellotti V (1998) Design for Privacy in Multimedia Computing and Communications Environments, in *Technology and Privacy: The New Landscape*. Agre and Rotenberg eds., MIT Press 63-98

6 Bellotti V, & Sellen A (1993) Design for Privacy in Ubiquitous Computing Environments, in *Proceedings of the Third European Conference on Computer-Supported Cooperative Work (ECSCW'93)*. Kluwer Academic Publishers, Milan 77-92

7 Boyle M (2005) Privacy in Video Media Spaces. PhD Dissertation, Department of Computer Science, Calgary, Canada

8 Boyle M, Edwards C, & Greenberg S (2000) The Effects of Filtered Video on Awareness and Privacy, in *Proceedings of the CSCW 2000 Conference on Computer Supported Cooperative Work* [CHI Letters 2(3)]. ACM Press 1-10

9 Boyle M and Greenberg S (2005) The Language of Privacy: Learning from Video Media Space Analysis and Design. *ACM Transactions on Computer-Human Interaction (TOCHI)*. 12 (2), June, 328-370, ACM Press

10 Brierley-Newell P (1995) Perspectives on Privacy, in *Journal of Environmental Psychology*, 15, Academic Press, New York, NY 87–104

11 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

12 Burkert H (1998) Privacy-Enhancing Technologies: Typology, Critique, Vision, in *Technology and Privacy: The New Landscape*, P Agre & M Rottenberg, Eds. MIT Press, Cambridge, MA 125–142

13 Clarke R (1994) The digital persona and its application to data surveillance, in *The Information Society*, 10:2. Taylor and Francis, New York, NY 77–92

14 Coutaz J, Bérard F, Carraux E, & Crowley J (1998) Early Experiences with the mediaspace CoMedi, in *IFIP Working Conference on Engineering for Human-Computer Interaction (EHCI'98)*, Heraklion, Greece

15 Crowley JL, Coutaz J, & Bérard F (2000) Things That See, in *Communications of the ACM*, ACM Press, vol 43, no 3, 54-64

16 Dourish, P (1993), Culture and Control in a Media Space, in Proceedings of the Third European Conference on Computer-Supported Cooperative Work (ECSCW'93), Kluwer Academic Publishers, Milan, pp. 125- 138.

17 Duval S, & Wicklund R (1972) *A theory of objective self-awareness*. Academic Press, New York, NY

18 Gaver W (1992) The Affordances of Media Spaces for Collaboration, in *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW'92)*, Toronto 17-24

19 Gavison R (1980) Privacy and the Limits of Law, in *Yale Law Journal*, 89:3 (January), The Yale Law Journal Company, New Haven, CT 421–471

20 Goffman E (1959) *The Presentation of Self in Everyday Life*. Doubleday Publishers, Garden City, NY

21 Grudin J (2001) Desituating Action: Digital Representation of Context, in *Human-Computer Interaction*, 16:2–4, Lawrence Erlbaum Associates, Hillsdale, NJ 269–286

22 Hall ET (1966) *Distances in Man: The Hidden Dimension*. Double Day, Garden City, NY

23 Harper RHR (1996) Why People Do and Don't Wear Active Badges: A Case Study, in *Computer Supported Cooperative Work: The Journal of Collaborative Computing*, Kluwer Academic Publishers, vol 4, no 4, 297-318

24 Harrison S, & Dourish P (1996) Re-place-ing Space: The Roles of Place and Space and Collaborative Systems, in *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW'96, Cambridge)*. ACM Press, New York, NY 67–76

25 Hixon R (1987), Privacy in a public society: Human rights in conflict. Oxford University Press, New York.

26 Hudson SE, & 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, MA 248-247

27 Jancke, G, Venolia, G D, Grudin, J, Cadiz, JJ, & Gupta, A (2001), Linking Public Spaces: Technical and Social Issues, in Proceedings of the ACM/SIGCHI Conference on Human Factors in Computing Systems (CHI 2001), Seattle, pp 530‑ 537.

28 Junestrand S, Keijer U, & Tollmar K (2001) Private and public digital domestic spaces, in *International Journal of Human-Computer Studies*, 54, 5 (May), Academic Press, New York, NY 753–778

29 Langheinrich M (2001) Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems, in *Proceedings of Ubicomp 2001*, Atlanta

30 Lee A, Girgensohn A, & Schlueter K (1997) NYNEX Portholes: Initial user reactions and redesign implications, in Pro*ceedings of the ACM/SIGGROUP Conference on Groupware (GROUP’97)* 385-394

31 Nardi BA, Whittaker S, & Bradner E (2000) Interaction and Outeraction: Instant Messaging in Action, in *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW’00)*, Philadelphia 79-89

32 Neustaedter C (2003) Balancing Privacy and Awarenes in a Home Media Space. Masters Thesis, Department of Computer Science, Calgary, Canada

33 Neustaedter C & Greenberg S (2003) The Design of a Context-Aware Home Media Space, in *Proceedings of UBICOMP 2003 Fifth International Conference on Ubiquitous Computing*. (Seattle, WA, USA), LNCS Vol 2864, Springer-Verlag 297-314

34 Neustaedter C, Greenberg S, & Boyle M (2006) Blur Filtration Fails to Preserve Privacy for Home-Based Video Conferencing. *ACM Transactions on Computer Human Interactions (TOCHI)*

35 Palen L, & 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

36 Root RW (1988) Design of a Multi-Media Vehicle for Social Browsing, in *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW’88)*, Portland, OR 25-38

37 Samarajiva, R (1997), Interactivity as Though Privacy Matters, in Technology and Privacy: The New Landscape, P. Agre & M. Rottenberg, Eds. MIT Press, Cambridge, MA.

38 Schwartz B (1968) The Social Psychology of Privacy, in *American Journal of Sociology*, 73:6, University of Chicago Press, Chicago, IL 741–752

39 Smith, I, & Hudson, S (1995), Low Disturbance Audio for Awareness and Privacy in Media Space Applications, in Proceedings of the third ACM international conference on Multimedia, San Fransisco, pp. 91-97.

40 Suchman, L (1987), Plans and Situated Actions: The Problem of Human-Machine Communication. Cambridge University Press.

41 Tang JC, Isaacs EA, & Rua M (1994) Supporting Distributed Groups with a Montage of Lightweight Interactions, in *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW'94)*, Chapel Hill, NC 23-34

42 Westin A (1967) *Privacy and Freedom*. Atheneum, New York, NY

43 Zhao QA, & Stasko JT (1998) Evaluating Image Filtering Based Techniques in Media Space Applications, in *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW'98)*, Seattle 11-18

About the authors

Michael Boyle
SMART Technologies, ULC

Michael Boyle is a Distinguished Developer in the software development group at SMART Technologies. He came to SMART in 2005 after he earned his Ph.D. in Computer Science from the University of Calgary. At SMART, Michael is focused on developing classroom-centered collaboration software for teachers and students. Usability and social workability of software inside and outside the classroom are his key areas of interest.

Carman Neustaedter
Kodak Research 1999 Lake Avenue
Rochester, NY 14580, USA
carman.neustaedter@kodak.com

Carman Neustaedter is a Research Scientist in the Computational Science & Technology Research group at Kodak Research Labs and an Adjunct Professor in the Department of Computer Science at the University of Rochester. Carman's research is in the areas of Human-Computer Interaction, Computer-Supported Cooperative Work, and Ubiquitous Computing, where he studies social culture to inform the design of technologies to support human activities. This research has involved studying, designing, and evaluating a wide range of computer technologies including email systems, instant messaging, video conferencing, digital photo software, calendars, online games, and pervasive location-based games. Carman holds a PhD in Computer Science from the University of Calgary, Canada. Labs

Saul Greenberg
Professor and iCore Chair
Human–Computer Interaction & Computer-Supported Cooperative Work
Department of Computer Science
University of Calgary
Calgary, Alberta, Canada T2N 1N4
saul.greenberg@ucalgary.ca

Saul Greenberg is a Full Professor in the Department of Computer Science at the University of Calgary. While he is a computer scientist by training, the work by Saul and his talented students typifies the cross-discipline aspects of Human–Computer Interaction, Computer-Supported Cooperative Work, and Ubiquitous Computing. He and his crew are well known for their development of toolkits enabling rapid prototyping of groupware and ubiquitous appliances, innovative and seminal system designs based on observations of social phenomenon, articulation of design-orientedsocial science theories, and refinement of evaluation methods. His research is well recognized. He holds the iCORE/NSERC/Smart Technologies Industrial Chair in Interactive Technologies. He also holds a University Professorship, which is a distinguished University of Calgary Award recognizing research excellence. He received the CHCCS Achievement Award in May 2007 and was also elected to the ACM CHI Academy in April 2005 for his overall contributions to the field of Human–Computer Interaction. Saul is a prolific author who has authored and edited several books and published many refereed articles, as listed at http://grouplab.cpsc.ucalgary.ca. He is also known for his strong commitment in making his tools, systems, and educational material readily available to other researchers and educators.