Privacy Implications of Surveillance Systems

Thommesen, Jacob; Andersen, Henning Boje

Published in:
Privacy Implications of Surveillance Systems

Publication date:
2009

Document Version
Early version, also known as pre-print

PRIVACY IMPLICATIONS OF SURVEILLANCE SYSTEMS

Authors: Jacob Thommesen (jact@man.dtu.dk) and Henning Boje Andersen (boje@man.dtu.dk)
DTU Management, Denmark.

Abstract

This paper presents a *model* for assessing the privacy 'cost' of a *surveillance system*. Surveillance systems collect and provide personal information or observations of people by means of surveillance technologies such as databases, video or location tracking. Such systems can be designed for various purposes, even as a service for those being observed, but in any case they will to some degree invade their privacy. The model provided here can indicate how invasive any particular system may be – and be used to compare the invasiveness of different systems. Applying a functional approach, the model is established by first considering the *social function* of privacy in everyday life, which in turn lets us determine which different *domains* will be considered as private, and finally identify the different types of *privacy invasion*. This underlying model (function – domain – invasion) then serves to explain the ways in which a technology-based surveillance system can affect the privacy of the observed. The model thus identifies a set of general characteristics (dimensions) of surveillance system that will determine the degree of invasiveness. The applicability of the model is demonstrated by analyzing a location-based system for airport passengers developed for a Copenhagen Airport, and the dimensions are used to explain user reactions to different services offered by the system.

This paper will present a model that identifies the main characteristics (dimensions) of a surveillance system that determine its degree of invasiveness. The model may assist in identifying critical aspects of a surveillance system to reduce "privacy costs" and thus to overcome the concerns of those who are the object of surveillance. But the model can also identify aspects of invasion that users may not be aware of or have difficulty in articulating. In this role, the model may be useful for the analysis of ethical aspects of different surveillance systems and may aid in foreseeing problems and reactions that may not appear until some time after implementing a system has been implemented.

The model is established by analyzing the notion of invasion of privacy, and invasion is in turn defined in terms of private domains. Finally, we suggest that private domains can be identified only by understanding what we use privacy for: the social function of privacy. We therefore consider these three steps in their logical order: the *social function* of privacy serving to identify the private *domains* and hence the various types of *invasiveness*.

What do we use privacy for?

Privacy can be conceived of as a means of ensuring our *security* (protection from harm), as a precondition for building *varied relationships* and for establishing and maintaining individual *autonomy*.

Security

When privacy is discussed in terms of *risk of abuse* (Hong et al., 2004), it is regarded as a means of ensuring *security* or protection against harm (Moor, 1997). Such protection is necessary because others may use sensitive information about you for their own purposes, which may be contrary to your interests. Information about your bank account may be used to steal your money, data retrieved from your health records may affect your insurance premium, and the unwelcome attention of a stalker may even constitute a risk of a physical assault.

In this perspective, protecting sensitive personal information and avoiding observation (e.g., stalking) is a means to reduce the risk of unwanted or even hostile actions by others. Concern for privacy is thus associated with emphasis on a hostile environment.

Social relationships and roles

But privacy concerns may not only prompt our seeking protection against abuse, but may also guide social relationships. We need privacy because in everyday life we have to conform to social norms of behavior. We have to maintain a public representation of ourselves, trying to control which parts of us are revealed to others in various contexts. We continually try to see ourselves in the eyes of others and to maintain an image or 'face' of ourselves that match their expectations (Goffman 1959).

While we thus conduct (much of) our social life as role-playing, we have a complementary need of a 'space' where we are not 'exposed'. The sociologist Goffman distinguishes metaphorically between being *onstage*, where we constantly manage the impression we make on others (impression management), and being *backstage* where we can relax – in *privacy* – and prepare our *onstage* performance (Andersen et al., 2007; Goffman, 1959).

Maintaining *intimate* relationships.

One privacy area to which we may retire and relax from most of the social norms is when we engage in *intimate* relationships with particular individuals (Fried, 1968; Gerstein, 1978). In doing so, we need not spend mental resources on *observing* ourselves, continuously assessing how we may be judged by a greater audience. Intimate relationships require *spontaneity*, which is incompatible with maintaining a 'face'. Such privacy may be provided by private space – e.g. a private home – but also by private conversations in a public place without being disturbed or eavesdropped upon; and if deprived of such privacy, our potential for maintaining intimate relations will be inhibited.

Varied relationships

Privacy also enables the maintenance of *varied* – and not necessarily intimate – relationships (Rachels, 1975). We form varied relationships by choosing what secrets to share with whom. We show different sides of ourselves in different relationships, and we tend to share more with close

friends than with 'looser' acquaintances. In order to maintain and form varied relationships we need to be able to distinguish between *different contexts* that imply different norms and expectations. We need to know how we are expected to behave, what the consequences are if we deviate from the norms, and how our behavior will be judged by others. But this varies depending on where we are and with whom. If we do not know who is watching us, we don't know how to behave and how our behavior may be judged.

For instance, when two close friends are joined by a casual acquaintance (Rachels, 1975), their behavior and the content of their conversation are very likely to change. They will not share the same *secrets* with the third persons as they did with each other, and they have to take into account how the newcomer will *interpret* their behavior and conversation – perhaps taking precautions to avoid misunderstandings.

Individual privacy and trust

Besides the need for privacy to protect varied relationships from a larger public, there is also a need for *individual* privacy. While some might expect people to share everything within intimate relationships, Fried argues that these should be build on *trust* and that trust requires individual privacy (Fried, 1968). Trust is an expectation about other people's behavior and thus based on incomplete knowledge. If we have some people under constant observation, we know all about their behavior – we don't need to trust them, and there is no opportunity to build trust.

The need for secrecy – and thus privacy – within intimate relationships can be illustrated by an example from a study of attitudes to location-enhanced technologies: a woman who does not want to be seen by her husband going into a particular shop because he thinks that she spends too much money there (Consolvo et al., 2005). Following Fried's argument, we may say that the husband's *observing* his wife would be an alternative to *trusting* her.

Private domains

Based on the understanding of the *role* of privacy sketched above, we will discuss a number of *domains* that are regarded as private – and thus potentially threatened by exposure. Still, it must be emphasized that privacy is not simply in opposition to maintaining social relations and identity and impression management, nor is privacy merely a 'refuge' where we protect ourselves from others by anonymity, secrecy and isolation (Gavison, 1980). Equally, any 'release of information' etc. is not per definition a loss or *cost*.

Rather, privacy should be understood as *complementary* to, and *interwoven* with, social identity. Privacy is implicit in impression management: it is what we don't share with everyone but choose to share *selectively* in order build social relations (Lahlou, 2008; Grimmelmann, 2008). This does not mean that we either keep others (strangers) out or let them in completely. We build social relations by trading 'bits' of privacy – not by dissolving boundaries.

Behavior, activities, decisions

Our behavior is critical to building and maintaining social relationships and thus to managing impressions. We adapt to various social contexts in which behavior is regulated by social norms, and we are judged by our ability to comply with those norms. We are therefore concerned how people judge *what we do*, and we use our past activities – *selectively* – to build a social identity (Lahlou, 2008).

Impression management depends on our ability to legitimate our activities, or keep those activities private that do not match the norms. We may prefer privacy – either in isolation or protected by anonymity – to indulge in habits or pleasures that do not match comfortably with our self-presentation in some social circles. Yet the same habits may be an acceptable part of our identity in another context. Thus, privacy of behavior depends on our ability to be aware of *who* is watching our behavior.

Private places

The privacy of behavior explains the common *spatial* concept of privacy, because it requires a physical realm where we expect to be 'let alone' (Warren & Brandeis, 1890). In our private home we can talk, behave and dress as we please, without being observed by others. Staying at home employs the strategy of *solitude* for maintaining privacy (Gavison, 1980).

We can also obtain some degree of privacy in *public* places: for example, we can protect ourselves by *anonymity* (Gavison, 1980); and we expect *norms* of privacy to prevent others from observing us closely or eavesdrop on our conversations; hence, public places – e.g. restaurants or cinemas – are fundamentally associated with some degree of privacy (Krämer, 1995; Altman, 1975).

This private sphere may be subject to different types of invasion, either as physical intrusion or as different kinds of observation (see the section 'Exposure – how can privacy be invaded?´, below).

Finally, places can also be private in another sense. They can be closely associated with particular activities, and the very knowledge of our location – and movements – can reveal what we are doing (Lahlou, 2008), e.g. going to the cinema or a gym, or visiting a bar or a particular shop.

Identity vs. anonymity

As already suggested, we can protect our privacy in public by maintaining *anonymity* (Gavison, 1980) - we don't mind other people seeing 'secret' sides of us in public, as a long as they don't know us and we do not expect to have anything to do with them later. Thus, we also guard our *identity* as a private area, and being identified may be an invasion in itself.

Personal information

The rise of the Internet have accentuated the *virtual* aspect of privacy, emphasizing that much *information* about us can be regarded as private, and that the acquisition of such information by others implies a loss of privacy.

One aspect of the informational privacy covers various categories of personal information that may be regarded as sensitive or embarrassing and thus should be considered private – because they are critical either to our *security* or our *social relations*. This includes racial and ethnic background, political or religious conviction, sexual preferences (Gavison, 1980; DeCew, 1986), personal health (e.g., health records) (Fried, 1968), criminal records and financial data (Posner, 1978).

However, informational privacy may also cover some of the other domains, especially information about our *behavior* or *activities*, e.g. "a person's remote and forgotten past" (Fried, 1968).

Personal relations and communication

We build and maintain relations by sharing secrets selectively, and we have to assume that our personal communication is not overheard by others. Even Posner, a privacy skeptic, argues that communications should be guarded as private, because treating it as *public* (thus allowing eavesdropping) would inhibit all communication (Posner, 1978). And Gerstein argues that it is wrong to observe a person against his will, but that it is far worse "where the victim of the invasion was submerged in an intimate relationship" (Gerstein, 1978).

Maintaining and establishing personal relations often occur in a public place, and when we engage in a private communication in public we normally estimate the degree of privacy: is anyone listening? Or are we protected by *anonymity*? Our estimation of privacy would be seriously jeopardized if we are in the vicinity of a camera or a listening device – and in particular if the observations or recordings could be related to our identity.

Exposure – how can privacy be invaded?

Based on the above discussion of various private domains we shall now summarize what can be considered as an *invasion* or a *loss* of privacy. We note in passing that we have deliberately wavered between the terms *exposure*, *loss* and *invasion*. We prefer the term *exposure* as the most neutral, while *invasion* both emphasizes the *spatial* metaphor and an *active* role played by another agent (an invader), whereas the term *loss* is *passive* and may have the connotation of a total loss – which is not intended here, of course.

We distinguish among three types of invasion (or loss or exposure): *intrusion*, *observation (intrusive vs. spying)* and *acquisition of personal information by others*.

1. The most obvious form of invasion is the *physical intrusion* of a private space such as the private home or other spatial demarcations, e.g. a workplace office or even a spot in a public park.
2. *Observation* is also form of invasion. If we are *aware* of being observed, we may speak of *intrusive observation* because we may change our behavior when we become aware of the observer's perspective and intentions. But *concealed* observation – *spying* – is also an invasion, since we are being observed, and 'judged' by someone 'out there', and an image or profile of us would be built (in someone's mind) that may affect our opportunities in the future. Gavison argues that the *attention* is a loss of privacy – the fact we have been 'singled out' and *identified*. Similarly, Introna argues that the *judgment and scrutiny by others* is an invasion (Introna, 1997). It should be emphasized that observation is not simply invasive in terms of acquiring information (see below). E.g., somebody spying on us in our homes through a telescope, may be regarded as invading our privacy – *even* if they fail to acquire new information (Gavison, 1980).
3. A third form of invasion, and one that is in focus when discussing privacy on the Internet, occurs when others *acquire personal information* about us. Such information could be abused, perhaps threatening our security, or it could affect our social relations.

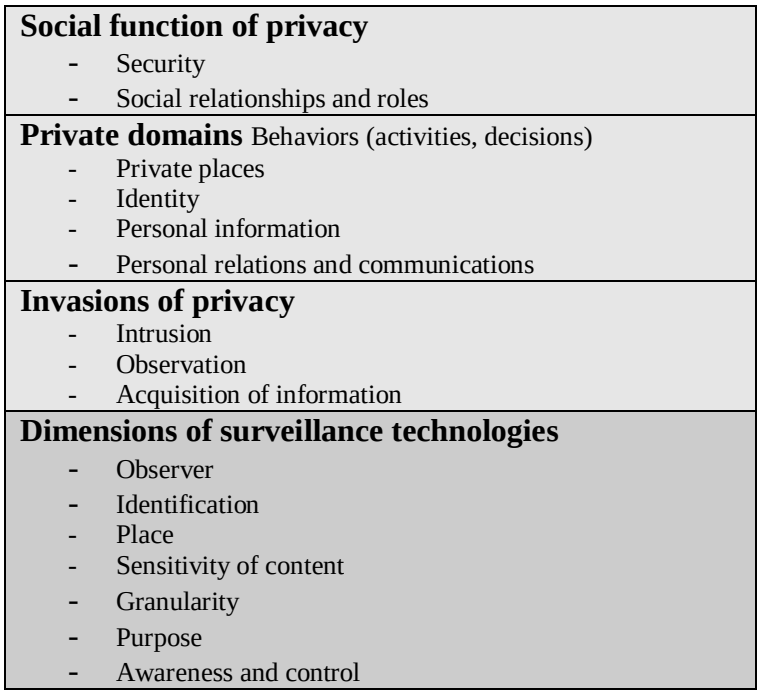

Figure 1. Overview of the model presenting the underlying concepts of *social function*, *private domains* and *types of invasions* as a basis for determining seven dimensions of surveillance technologies.

Invasive technologies – seven dimensions

Loss of privacy is often associated with technological development that offers new or improved opportunities for providing and collecting information and observations. Yet, the degree of invasion is not determined by the technology itself, but depends on its application in a *system* that provides surveillance for someone (the *observer*) for some *purpose*.

And the threat is not limited to the paradigmatic surveillance where someone is watched by somebody else. Rather, invasions may often be unexpected consequences of technology-based services designed to support communication and social relations. For instance, mobile phones may provide the caller with information about the receiver's current situation to reduce interruptions (Khalil & Connelly, 2006); verbal communication may be augmented by video that reveals more than intended (Short et al., 1976); and friends may share personal information – including location – via Online Social Networks such as Facebook, without being quite aware of the extent of the audience (Grimmelmann, 2008; Lahlou, 2008) – to name but a few prominent examples.

Rather than focusing on the privacy aspects of one particular technology or application, this paper proposes a general model that allows us to compare the privacy implications of different 'surveillance systems'. Technologically different systems may have many critical characteristics in common – e.g. the *observer* and *purpose* of the surveillance. Therefore, invasions associated with a particular technology – e.g. video and RFID – are better understood in terms of basic private domains such as those presented in the previous section.

The model we propose include a number of dimensions that affect the degree of invasion and that correspond to some of the *factors* identified in a number of studies of users' willingness to disclose information (Adams, 2000; Lederer et al., 2003; Consolvo et al., 2005; Khalil & Connelly, 2006). These studies emphasize the receiver identity or the 'who' (the *observer*) and the 'usage' or 'why' (*purpose*). *Level of detail* (*granularity*) and *location* (Consolvo et al., 2005) are also relatively well defined, while other factors such as *context* (Adams, 2000) and *situation* (Lederer et al., 2003) are more difficult to specify, but might be indicated by the *type of place*. One study also considers whether the participants 'have company', and whether they are engaged in 'conversation' (Khalil & Connelly, 2006), which is highly relevant according to our definition of the role of privacy, but not useful as characteristics of the surveillance system itself.

1. The observer – who wants the information?

Bearing in mind the *role* of privacy the degree of invasion obviously depends largely on who the observer is. One can distinguish between different types of observers: *institutions* (both public authorities and private companies) and *people* who are somehow *socially related* to the object of surveillance.

Institutional surveillance will primarily affect the *security* aspect, whereas *relational surveillance* will affect the observed subject's potential for presentation management. The character of invasion associated with *state* surveillance (Big Brother) differs from surveillance by private companies (Little brother), but this difference largely depends on other factors such as the *purpose* of the observation, and the *degree of identification* (negation of anonymity).

As for *relational surveillance*, the loss of privacy will generally decrease, the closer the relationship with the observer, because we already share more with those we know best, e.g., more with a significant other or family member than with a boss or a stranger (Khalil & Connelly, 2006). Yet we can still lose privacy to a significant other, as discussed previously (see the section 'Individual privacy and trust').

2. Degree of personal identification

The loss of privacy also depends strongly on the degree to which a person is identified, since identification disables one of our basic strategies for privacy protection: *anonymity* (Gavison, 1980). So, a tracking system is more invasive than camera surveillance in a public place to the extent that the former and not the latter has information about people's identity.

Identification may be derived from other types of information, e.g. databases with narrow group identifiers or RFID-applications attached to items that are closely associated with a particular individual.

3. Setting – type of place

The loss of privacy also depends on where the surveillance takes place, since we fundamentally perceive places in terms of the degree of privacy they afford (cf. above).). Surveillance will be more invasive in a private home than in a public square, since there will be privacy 'to lose'. But there are many categories in-between the two extremes (Grandhi et al., 2005).

4. Sensitivity of content: information and observations

Obviously, the degree of invasion also depends on the information and observations collected by the surveillance system. On the one hand, much 'literal' information can be classified in degrees of sensitivity (see section on 'Personal information'). On the other hand, particular surveillance technologies may also invade other *private domains* in a more complex sense than simply acquiring information.

Thus a *camera* can observe behaviour (activities cf. above) and personal relationships, and provide nonverbal cues – e.g. facial expression, body language – that may reveal feelings and reactions that were not intended for a wider audience.

Listening devices are designed to record conversation – which is in itself a highly private domain (cf above) – and may thus disclose any type of sensitive information.

Location-based systems can indicate *activities* associated with certain locations, and movements between different places may also suggest something about personality and intentions. Furthermore, co-locations with other people indicate social relations.

5. Surveillance technologies - granularity

Focusing on the particular surveillance technologies, the degree of invasion increases with the technology's degree of accuracy: a low resolution camera would not register facial expression, and a superficial tracking system (low precision, infrequent registration) can only give a very vague location and 'blurred' movements.

6. The 'purpose' of observation

The loss of privacy also depends on the *purpose* of a surveillance system, which is often related to the *subject* (the observer). E.g. *institutional surveillance* by the state is often established for *security* or *control*, surveillance by private companies normally carried out for *commercial* purposes, while *relational surveillance* is established for the purpose of *social awareness*: sharing information with friends, contacts and relatives, seeing each other on video or keeping track of each other's whereabouts.

The purpose affects the degree of privacy invasion, because it determines the way the information is being *interpreted* – and *judged* (Introna, 1997). Certain activities or words may be critical and provoke scrutiny and interpretation, and those being observed, if aware of the surveillance, will modify their behaviour to avoid being "caught" or exposed It must be emphasized that the focus here is on how the purpose affects the *loss of privacy*, which must be separated from the effect on the users' *accept* of surveillance. The perceived benefits of a particular surveillance system may lead users to accept it even at a considerable loss of privacy, based on a cost-benefit *trade-off* (Ng-Kruelle et al., 2002). But it is important to treat the questions separately, since the users' loss of privacy remains and is not reduced by their accept.

7. Awareness and control

Whether *the observed subject* is *aware* of the observer is crucial to the degree of invasion, because our impression management – in terms of controlling behaviour and disclosure of information – is directed towards the perceived audience. We maintain social relations by sharing information *selectively*.

Thus, some online social networks are invasive, since users cannot control the audience, or the actual audience turns out to be larger than expected. If a surveillance system does not provide adequate cues indicating the actual audience (Grimmelmann, 2008; Tsai et al., 2009; Hansen et al., 2009), people may be led to unintended disclosure – as when pictures shared with friends are viewed by a potential employer.

Besides awareness of the audience, loss of privacy also depends on the users' *control* over the disclosure – the ability to be selective. However, the *control* dimension should primarily be applied to identify problems – increased invasiveness due to lack of control – rather than treated as a recommendation of sophisticated control features, since these often do do not match the more subtle social mechanisms they were meant to support.

Observer	*Institutional* (public, private) *Relational* (closeness/degree of intimacy)
Identification	*Individual, group, anonymous*
Place	Private vs. public (degrees)
Sensitivity of content (data, activities)	Personal data (categories) Sensitive behaviors
Granularity	Level of detail, temporal extension
Purpose	Safety, security, commercial, relational
Awareness, control	overt vs. hidden surveillance; degree of control

Table 1. Dimensions of surveillance systems affecting their degree of invasiveness

Tracking airport passengers – an example

The applicability of the model can be demonstrated by using the dimensions outlined above to analyze privacy implications of a location-based service (the Gatecaller) being developed for passengers in Copenhagen Airport (Hansen et al., 2009). The service, which is based on RFID and Bluetooth, was designed, first, to reduce flight delays due to passengers not arriving in time for boarding, in which case their luggage must be unloaded with ensuing delayed departure, and second, to reduce passenger anxiety and uncertainty about being late. Furthermore, the airport expected commercial benefits when passengers spend more time in the shopping area and less time waiting in front of information screens to catch their gate and boarding time and, similarly, less 'buffer time' waiting at the gate. The application offers three different services: a basic service and two additional features that are specified as optional based on the expectation that these services have increasing implications for privacy (see discussion below).

Two surveys have been carried to elicit travelers' attitudes to the Gatecaller services and associated privacy issues. The first is a web-based survey, and the other is a questionnaire survey of passenger reactions to the first trials with the prototype system. The web survey, from which most of the following is derived, invited respondents to make a cost-benefit trade-off (Ng-

Kruelle et al., 2002), balancing the perceived privacy cost of the service against the expected gains. While this paper focuses on the 'cost side' of this trade-off, both the web survey and the field trial confirmed that there was indeed a perceived benefit.

A test trial was carried in cooperation with an airline (Scandinavian Airlines System) inviting passengers on two charter flights to in a pilot trial by carrying an RFID badge on their handbag between check-in and till they reached their gate and to register their mobile phone. Arriving at the gate, the volunteers were asked to fill out a short questionnaire on their experience. One of the questions was: "Has it made you feel more secure that the gate personnel now may find you if you are late", and as can be seen from the answers (Table 2), a majority (60 %) feels to some degree or to a large degree more secure.

[N = 76]	No, not at all	No, hardly at all	Yes, to some degree	Yes, to a large degree
	20 %	20 %	39 %	21 %

Table 2. "Feeling more secure now?"

Web survey indicating varying degrees of invasion

A web survey was carried out prior to field trials to assess potential users' attitude to the service and especially their perceptions of privacy 'costs'. Announcements of and invitation to the survey was posted on a popular travel website. Since the validity of web surveys is often undermined by the fact that samples are based on self selection, various measures were taken to appeal to different groups of respondents. The questions and lead-up texts were deliberately phrased to attract in equal measure respondents who are keen to use new IT-technology as well as those who are concerned about privacy issues – and thus to reduce the risk that the sample would be biased towards either the 'tech savvy' or the 'privacy paranoids' (see Figure 2). Furthermore, the invitation was also designed to attract the 'lukewarm' by giving respondents the opportunity to participate in a draw for a modest reward (10 gift cards, each at $58).

"Do you think you might like to use Gatecaller or are you, perhaps, a bit skeptical of a technology that can track your location within an airport? In either case, we'd like your opinion on this new service and on tracking technologies in general."

Figure 2. Invitation text for web survey.

After a fairly detailed description of the service respondents are asked whether they would use the proposed service. Those who answer 'no', are asked to indicate their reasons for declining the service. The questions thus invites the respondents to make an informed choice and thus to consider whether they are so concerned that they would decline the service. They are asked not merely about their attitude, but invited – indirectly – to rate the privacy cost against potential benefits. As can be seen in the following, only a small proportion of respondents are concerned about the basic Gatecaller service, but results indicate increasing concerns over the two additional services, and the model presented above can be used to explain some of these differences.

1) Automatic, location-based services

The respondents were very positive towards the basic service (the GateCaller) which provides *mobile* information to the passenger's cell phone about gate number and boarding time, as well as an estimation of the time required to reach the gate. A majority of respondents (83 %; N =

503) said ‘yes’ and 13 % ‘maybe’ to using this service which is based on an *automatic* registration of the passenger’s current location and flight information. Only 4 % said ‘no’.

2) Locating delayed passengers – some reluctance

A majority (67 %) also wanted an additional service allowing *gate personnel* to locate and possibly call them, should they be in danger of missing their flight. However, one out of four (26 %) preferred to stick with the basic version, thus rejecting this additional service. Asked for their reasons for doing so, most of them (72 %) indicated that they don’t need it, while 22 % don’t want others to see their location, and 15 % express concern about data misuse (n = 125; reply options non-exclusive).

This reluctance to accept the ‘locator’ service, partly based on privacy concerns, indicates that it is considered more *invasive* than the basic service, and this difference may be explained by referring to some of the dimensions presented in this paper.

It is more invasive along the *identity* dimension. Already, the basic service undermines the passengers’ anonymity which is a basic privacy protection in a public place like the airport. But the basic service only requires *group* identification as members of a passenger list, while the ‘locator’ service requires *individual* identification.

It is also more invasive in the *observer* dimension, since it adds a human observer to the automatic, impersonal observer in the basic version. In terms of social relations, the passenger’s location and movements will now be watched by a *stranger* who, moreover, will possibly meet her at the gate.

The *sensitivity of content* is also increased by the human observer who may interpret location and movements as information about the passenger’s activities (depending on the granularity provided). Location data will now be associated with *meaning*. Is the passenger shopping (in which shop) or resting at a café or in a waiting area? Rather than speculating on what ‘snoopy’ observers might interpret from passenger locations – a subject ripe with anecdotes and over-interpretations – we may focus on the meaning that the gate personnel associate with locations and movements when guided by their professional *purpose*. Their task is to board the passengers in time for departure, and they will monitor them (their dots on the screen) in this perspective: are they on their way to the gate or ‘straying’ in a shopping area in the opposite direction? Passengers staying at a bar may receive extra attention, since they are rumored to cause delay – and this professionally motivated attention may also imply judgments concerning drinking habits.

Table 3. Compares 'basic' with 'locator' service along four privacy dimensions.

Dimension	Basic Gatecaller	‘Locator’
Identification	Passenger list	Individual
Observer	Automatic system	Gate personnel (stranger)
Sensitivity of information	neutral location data	Places indicating activities
Purpose	Not applicable (no human observer	‘Are they responsible?’

3) Family monitoring – more skepticism

The respondents were more skeptical towards another additional service, letting the passenger revealing his or her location to *friends* or *relatives* via real-time upload of location data to a server. This could be used by parents to traveling teenagers or relatives to traveling elderly or disabled passengers who might feel insecure when alone in the airport.

Well over a third (39 %) of the respondents would use this 'family monitoring' service – seeing or being seen by a relative or friend – while an equal proportion (39 %) rejected it, most of them (70 %) indicating that 'people should be left to walk around' (i.e. a privacy concern), while 40 % stated that they don't need the service.

This result suggests that the 'family monitoring' service is considered even more invasive than the 'locator' service. This may also be – partly – explained by the model since the two services differ along at least two dimensions: *granularity* and *observer*. Thus the 'family monitoring' service is more invasive in the technical dimension, since it is continuous and extends through the entire stay at the airport, whereas the basic service only focuses on the location around the time of boarding.

However, it also differs significantly along the *observer* dimension, since the 'stranger' is now replaced by a relative or friend, thus converting the *institutional* surveillance to a social 'awareness' service – comparable to a Social Network System like Facebook. This difference is more ambiguous, since one might expect the closer social relationship to be less invasive – and thus balance the effect of increased granularity. Nevertheless, this 'intimate observer' also invades *individual privacy*, and locations may be more ripe with meaning, since relatives and friends may be attentive to more – and other – details than the gate personnel.

Conclusion

The privacy model presented here has been developed to help in assessing the privacy implications of a surveillance system and in comparing different systems. It can inform the design of empirical studies of user attitudes and levels of acceptance, for instance, by suggesting framing of questions that direct attention to aspects of use and types of privacy loss that may not be immediately distinct. The main benefit of the model is therefore its ability to support analysis of technology-based services by considering the basic *roles* of privacy, and the consequences for the *private domains*.

Reference List

Adams, A. (2000). Multimedia information changes the whole privacy ballgame. In (pp. 25-32).

tenth conference on Computers, freedom and privacy: challenging the assumptions.

Altman, I. (1975). *The environment and social behavior*. Monterey: Brooks/Cole Publishing Company.

Andersen, H., Brante, T., & Korsnes, O. (2007). *Leksikon i sociologi*. (2nd ed.) København: Akademisk Forlag.

Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). Location Disclosure to Social Relations: Why, When, & What People Want to Share. In SIGCHI conference on Human factors in computing systems.

DeCew, J. W. (1986). The scope of privacy in law and ethics. *Law and Philosophy, 5*, 145-173.

Fried, C. (1968). Privacy. *Yale Law Journal, 77,* 475-493.

Gavison, R. (1980). Privacy and the limits of the law. *Yale Law Journal, 89*, 421-471.

Gerstein, R. S. (1978). Intimacy and privacy. *Ethics, 89,* 76-81.

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

Grandhi, S. A., Jones, Q., & Karam, S. (2005). Sharing the Big Apple: A Survey Study of People, Place and Locatability. In (pp. 1407-1410). CHI 2005, Portland, Oregon, USA: ACM.

Grimmelmann, J. T. (2008). Facebook and the Social Dynamics of Privacy. *NYLS Legal Studies Research Paper No.08/09-7*.

Hansen, J. P., Alapetite, A., Andersen, H. B., Malmborg, L., & Thommesen, J. (2009). Location-based services and privacy in airports. In INTERACT 2009.

Hong, I., Ng, J. D., Lederer, S., & Landay, J. A. (2004). Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. In DIS2004 - Designing Interactive Systems.

Introna, L. D. (1997). Privacy and the Computer: Why We Need Privacy in the Information Society. *Metaphilosophy, 28,* 259-275.

Khalil, A. & Connelly, K. (2006). Context-aware Telephony: Privacy Preferences and Sharing Patterns. In (pp. 469-478). CSCW'06.

Krämer, B. (1995). Classification of generic places: Explorations with implications for evaluation. *Journal of Environmental Psychology, 15,* 3-22.

Lahlou, S. (2008). Identity, social status, privacy and face-keeping in digital society. *Social Science Information, 47,* 299-330.

Lederer, S., Mankoff, J., & Dey, A. (2003). Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In CHI 2003: NEW HORIZONS.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *Computers and Society, 27.*

Ng-Kruelle, G., Swatman, P. A., Rebne, D. S., & Hampe, J. F. (2002). Price of Convenience: Dynamics of Adoption Attitudes and Privacy Sensitivity Over Time. In CollECTeR (Conference on Electronic Commerce) 2002, Melbourne, Australia.

Posner, R. A. (1978). The right of privacy. *Georgia Law Review, 12,* 393-422.

Rachels, J. (1975). Why privacy is important. *Philosophy and Public Affairs, 4,* 323-333.

Short, J., Williams, E., & Christie, B. (1976). *The Social Psychology of Telecommunications*. London: John Wiley & Sons.

Tsai, J. Y., Kelley, P., Drielsma, P., Cranor, L., Hong, J., & Sadeh, N. (2009). Who's viewed you?: the impact of feedback in a mobile location-sharing application. In (pp. 2003-2012). Boston, MA, USA.

Warren, S. D. & Brandeis, L. D. (1890). The Right of Privacy. *Harvard Law Review, 4,* 193-220.